Data Security in Photonic Information Systems using Quantum Based Approaches

Patrick Joseph Clarke

Submitted for the degree of Doctor of Philosophy

Heriot-Watt University

School of Engineering and Physical Sciences

March 2013

Abstract

The last two decades has seen a revolution in how information is stored and transmitted across the world. In this digital age, it is vital for banking systems, governments and businesses that this information can be transmitted to authorised receivers quickly and efficiently. Current classical cryptosystems rely on the computational difficulty of calculating certain mathematical functions but with the advent of quantum computers, implementing efficient quantum algorithms, these systems could be rendered insecure overnight. Quantum mechanics thankfully also provides the solution, in which information is transmitted on single-photons called qubits and any attempt by an adversary to gain information on these qubits is limited by the laws of quantum mechanics.

This thesis looks at three distinct different quantum information experiments. Two of the systems describe the implementation of distributing quantum keys, in which the presence of an eavesdropper introduces unavoidable errors by the laws of quantum mechanics. The first scheme used a quantum dot in a micropillar cavity as a single-photon source. A polarisation encoding scheme was used for implementing the BB84, quantum cryptographic protocol, which operated at a wavelength of 905 nm and a clock frequency of 40 MHz. A second system implemented phase encoding using asymmetric unbalanced Mach-Zehnder interferometers, with a weak coherent source, operating at a wavelength of 850 nm and pulsed at a clock rate of 1 GHz. The system used depolarised light propagating in the fibre quantum channel. This helps to eliminate the random evolution of the state of polarisation of photons, as a result of stress induced changes in the intrinsic birefringence of the fibre. The system operated completely autonomously, using custom software to compensate for path length fluctuations in the arms of the interferometer and used a variety of different single-photon detector technologies. The final quantum information scheme looked at quantum digital signatures, which allows a sender, Alice, to distribute quantum signatures to two parties, Bob and Charlie, such that they are able to authenticate that the message originated from Alice and that the message was not altered in transmission.

Acknowledgements

I would firstly like to thank my supervisor Prof. Gerald S. Buller whose support and guidance has helped me endlessly over the last few years. I am very grateful for being given a once in a lifetime opportunity. I would like to thank Dr. Robert Collins for his help, dedication and patience over the course of my PhD. I would also like to thank the more "senior" members of the group who deserve a special mention, Dr. Aongus McCarthy and Dr. Ryan Warburton. I would also like to thank the present and past members of the Photon Counting group, Dr. Phil Hiskett, Dr. Nils Krichel, Frauke Izdebski, Silvia Butera, Giuseppe Intermite, Nathan Gemmell, Ximing Ren, Agata Pawlikowska, Aurora Maccarone, Dr. Peter Vines and Ross J. Donaldson.

I would like to thank some of my collaborators that I have worked with; Prof. Robert Hadfield and Dr. Erika Andersson from Heriot-Watt, Dr. John Jeffers from the University of Strathclyde, Prof. Paul Townsend from the Tyndall National Institute in Ireland, Prof. Maurice Skolnick and Prof. Mark Fox from the University of Sheffield and Prof. Mark Hopkinson at the EPSRC National Centre for III-V Technologies in Sheffield. I would also like to thank Vedran Dunjko from Heriot-Watt University and María-José García-Martínez at the Department of Information Processing and Coding in CSIC in Madrid. I would also like to thank my former office mates, Ruth Livingston and Will Ramsay. I would also like to thank Mr. Jun Liu for his help.

My family deserve a very special thanks, my sisters Ita and Joanne, and my Mum and Dad, who have been a constant source of support and encouragement throughout my life. Finally to you Lining, thanks for keeping me going through the hard times, I couldn't have done it without you!

ACADEMIC REGISTRY

Research Thesis Submission

Name*:*	Patrick Joseph Clarke		
School/PGI:	School of Engineering and Physical Sciences		
Version: *(i.e. First, Resubmission, Final)*	Final	Degree Sought (Award **and** Subject area)	PhD Physics

Declaration

In accordance with the appropriate regulations I hereby submit my thesis and I declare that:

1) the thesis embodies the results of my own work and has been composed by myself
2) where appropriate, I have made acknowledgement of the work of others and have made reference to work carried out in collaboration with other persons
3) the thesis is the correct version of the thesis for submission and is the same version as any electronic versions submitted*.
4) my thesis for the award referred to, deposited in the Heriot-Watt University Library, should be made available for loan or photocopying and be available via the Institutional Repository, subject to such conditions as the Librarian may require
5) I understand that as a student of the University I am required to abide by the Regulations of the University and to conform to its discipline.

* *Please note that it is the responsibility of the candidate to ensure that the correct version of the thesis is submitted.*

Signature of Candidate*:*		Date:	

Submission

Submitted By *(name in capitals):*	PATRICK JOSEPH CLARKE
Signature of Individual Submitting:	
Date Submitted:	

For Completion in the Student Service Centre (SSC)

Received in the SSC by *(name in capitals):*			
Method of Submission *(Handed in to SSC; posted through internal/external mail):*			
E-thesis Submitted ***(mandatory for final theses)***			
Signature:		Date:	

Contents

List of Journal Publications

Journal Publications

P.J. Clarke, R.J. Collins, V. Dunjko, E. Andersson, J. Jeffers and G.S. Buller, *"Experimental demonstration of quantum digital signatures using phase–encoded coherent states of light"*, Nature Communications, **3** Article ID 1174 (2012)

P.J. Clarke, R.J. Collins, P.A. Hiskett, M.-J. García-Martínez, N.J. Krichel, A. McCarthy, M.G. Tanner, J.A. O'Connor, C.M. Natarajan, S. Miki, M. Sasaki, Z. Wang, M. Fujiwara, I. Rech, M. Ghioni, A. Gulinatti, R.H. Hadfield, P.D. Townsend and G.S. Buller, *"Analysis of detector performance in a gigahertz clock rate quantum key distribution system"*, New Journal of Physics **13**(7), Article ID 075008 (2011)

P.J. Clarke, R.J. Collins, P.A. Hiskett, P.D. Townsend and G.S. Buller, *"Robust GHz fiber quantum key distribution"*, Applied Physics Letters, **98**(13), Article ID 131103 (2011)

R.J. Collins, **P.J. Clarke**, V. Fernandez, K.J. Gordon, M.N. Makhonin, J.A. Timpson, A. Tahraoui, M. Hopkinson, A.M. Fox, M.S. Skolnick and G.S. Buller, *"Quantum key distribution system in standard telecommunications fiber using a short wavelength single photon source"*, Journal of Applied Physics, **107**(7), 073102 (2010)

Conference Publications

P.J. Clarke, R.J. Collins, V. Dunjko, J. Jeffers, E. Andersson, G.S. Buller, *"An Experimental Demonstration of Quantum Digital Signatures"*, Photon 12, Durham, UK (September 2012)

R.J. Collins, **P.J. Clarke**, V. Dunjko, J. Jeffers, E. Andersson and G.S. Buller, *"Experimental demonstration of quantum digital signatures"*,Quantum Information and Measurement (QIM), Berlin, Germany (March 2012)

P.J. Clarke, R.J. Collins, P.A. Hiskett, P.D. Townsend, G.S. Buller*"An analysis of single–photon detectors in a gigahertz clock rate robust quanrtum key distribution system"*,Single Photon Workshop 2011, Braunschweig, Germany (June 2011)

P.J. Clarke, R.J. Collins, A. McCarthy, N.J. Krichel, M.J. García-Martínez, M.G. Tanner, J.A. O'Connor, C.M. Natarajan, S. Miki, M. Sasaki, Z. Wang, I. Rech, M. Ghioni, A. Gulinatti, P.A. Hiskett, R.H. Hadfield, P.D. Townsend, G.S. Buller, *"An Analysis of Single–photon detectors in an environmentally robust gigahertz clock rate quantum key distribution system"*, CLEO QELS 2011, Baltimore, USA (May 2011)

P.J. Clarke, R.J. Collins, P.A. Hiskett, N.J.Krichel, C.M. Natarajan, R.H. Hadfield, P.D. Townsend and G. S. Buller,*"Environmentally robust GigaHertz clock rate quantum key distribution"*, QEP 19, Southampton, UK (August 2010)

R.J. Collins, **P.J. Clarke**, P.A. Hiskett, V. Fernandez, M.–J. Garcia–Martinez, M.N. Makhonin, J.A. Timpson, M. Hopkinson, A.M. Fox, M. Skolnick, and G.S. Buller *"Short wavelength quantum key distribution in telecommunications optical fiber"*, NIST Workshop on Single and Entangled Photons: Sources, Detectors, Components and Applications, Boulder, USA (November 2009)

Chapter 1
Introduction

1.1 Introduction

Cryptography, the science of secret writing, is already several millennia old and was known and used to good effect by the ancient Spartans and Greek civilisations. Cryptography now plays a vital part in secure global communications in the world today and is used by governments, international commerce and military organisations [1].

In 1917, work by Gilbert Vernam made an important contribution to field of cryptography with the discovery of the one-time pad [2]. This encryption method combines a plaintext message with a pseudorandom key via Boolean arithmetic, and when the key is the same length of the message is proven to be impossible to crack by pioneering work developed by Claude Shannon [3].

Prior to the 1970's encryption required that communicating parties shared a private key in advance to encrypt and decrypt messages. In such a scheme, where the same key is used to encrypt and decrypt, the secure and efficient distribution of keys was an issue. In 1976 the problem of secure key distribution was overcome by Whitfield Diffie and Martin Hellman by the protocol that bears their name [4]. Diffie-Hellman key exchange also allowed the possibility of signing documents using digital signatures, in which messages transmitted could be verified to be authentic. For cryptography appylications it meant that by using the principle of one-way functions, a shared secret key could be established between two communicating parties without a key being exchanged in advance. This so called secret key cryptography, which used the same key for encryption and decryption, was later replaced by public key cryptography using different keys for the encryption and decryption process following on from the work of Ron Rivest, Adi Shamir, and Leonard Adleman (RSA). The widely used cryptographic protocol called RSA relies on the infeasibility of reversing certain one-way mathematical functions [5]. Currently the time and the amount of computational resources required to invert these functions makes these protocols secure [6] but a breakthrough in mathematical science or with the advent of quantum computing which could implement Shor's factoring algorithm [7] could render current cryptosystems insecure.

In the late 1970's the meeting of ideas in quantum information and public key cryptography lead to the birth of quantum cryptography, whose security could be guaranteed by fundamental laws of quantum mechanics. Information could be encoded on single-photons of light and any attempt by unauthorised parties to learn the state of an encoded photon would disturb the state as a direct consequence of the Heisenberg uncertainty principle [8]. This concept enabled the distribution of quantum cryptographic keys whose security could be verified. Bennett's and Brassard's BB84 cryptographic protocol [9] was the first to be fully described and subsequently implemented, and paved the way for further research in the area.

This thesis will look at various quantum information experiments which have been implemented in the research group, with this chapter serving as a general introduction and brief outline.

Chapter 2 will begin by giving a brief overview of classical cryptography, describing some early substitutional encryption methods and eventually leading on to describe public key cryptography (PKC). The weakness of PKC, which relies on one-way functions, will be described and leads to a description of quantum key distribution which seeks to eliminate this problem. Several quantum cryptographic protocols will be described including the widely used BB84 protocol which is used extensively in the experimental sections of this thesis. The second part of Chapter 2 looks at some of the technology required to implement a quantum key distribution (QKD) system including the generation and detection of single-photons.

Chapter 3 will describe a QKD system using semiconductor quantum dots embedded in a micropillar cavity as a source of single-photons emitting at a wavelength of 895 nm. The system implements the BB84 protocol using polarisation encoding, with the quantum channel composed of standard telecommunications fibre.

Chapter 4 will describe an environmentally robust gigahertz QKD system operating at a wavelength of 850 nm, tested using a variety of single-photon detector technologies. Using optical depolarising techniques on a weak coherent source, birefringence effects in the quantum fibre link can be removed, therefore removing the necessity of complicated and costly polarisation monitoring equipment.

Chapter 5 will introduce a topic which is slightly different from, but related to that described in previous chapters. Digital signatures, which enable communicating parties to authenticate messages and allow verification that the messages have not been altered in transmission, will be introduced. Like classical encryption schemes, these rely on the unproven computational difficulty of reversing certain one-way functions. Quantum digital signatures can replace these classical one-way functions with the quantum mechanical equivalent of these functions. The amount of classical information that can be gleamed from the generated quantum state is restricted by the laws of quantum mechanics. Chapter 5 will also describe an experimental demonstration using two recipients and one sender employing similar experimental techniques to those used in previous experimental chapters.

Chapter 6 will serve as a general conclusion to the thesis, briefly summarising each chapter and highlighting the key results and discoveries. It will also outline possible future work and research directions which are worth pursuing.

References

[1] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone, "*Handbook of applied cryptography"* 1997: CRC.

[2] G.S. Vernam, "*Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications"*. American Institute of Electrical Engineers, Transactions of the, 1926. **XLV**: p. 295-301.

[3] C. Shannon, "*A mathematical theory of communication"*. Bell Labs System Technical Journal 1948. **27**(1): p. 379-423, 623-656.

[4] W. Diffie and M. Hellman, "*New directions in cryptography"*. IEEE Transactions on information Theory, 1976. **22**(6): p. 644-654.

[5] R. Rivest, A. Shamir, and L. Adleman, "*A method for obtaining digital signatures and public-key cryptosystems"*. Communications of the ACM, 1978. **21**(2): p. 120-126.

[6] J. Katz and Y. Lindell, "*Introduction to modern cryptography"* 2008: Chapman & Hall.

[7] P.W. Shor. "*Algorithms for quantum computation: discrete logarithms and factoring"*. in *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*. 1994.

[8] W. Heisenberg, "*Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik"*. Zeitschrift für Physik A Hadrons and Nuclei, 1927. **43**(3): p. 172-198.

[9] C.H. Bennett and G. Brassard. "*Quantum cryptography: Public key distribution and coin tossing"*. in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. 1984. Bangalore, India.

Chapter 2

Introduction to Cryptography and Equipment

2.1 Introduction

The first part of this chapter gives a brief overview of classical cryptography and describes the development towards quantum key distribution (QKD). The second part gives a description of some of the technologies required for QKD including the generation and detection of single-photons.

2.2 Overview of Classical Cryptography

Cryptography deals with the art of converting ordinary information called *plaintext* into seemingly unintelligible gibberish using a process called encryption. Decryption converts the ciphertext back into plaintext. A cipher is the algorithm that describes the encryption and decryption process. The cipher is controlled by the algorithm and the secret key. This key should only be available to authorised parties enabling messages to be sent securely.

The ability to securely transmit information between two parties has always been a desire for many civilisations. Over the course of history the secure transmission of messages became more important with the increasing quest to achieve military superiority over other nations. The ancient Greeks wrote messages on wooden tablets and then covered them with wax so as to appear that there was no information contained on the tablet. It was the Spartans who established the first system of cryptography to be used in warfare. They invented a device called a scytale which consisted of a wooden staff and a strip of papyrus wrapped around it. The secret message would be written on the papyrus from left to right and then unwound. The letters on the strip do not make sense unless it is wrapped around a staff of the same thickness of the first. This was a form of a transposition cipher in which the letters of the message are simply rearranged to form an anagram [1].

The Romans were the first to use substitution ciphers, called the Caesar Cipher and named after Julius Caesar. This technique was used by him to communicate with his generals. The messages were written using a cipher in which the plaintext letters were replaced by letters standing a certain number places further down the alphabet (Table 2.1 shows a shift of three). Although easy to encrypt it was also easy to decrypt by

unauthorised parties by the technique of frequency analysis which relies on the fact that certain letters in the alphabet are repeated more often than others.

Plaintext	*a*	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
Cipher	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Table 2.1. Caesar Cipher implemented using a shift of 3.

2.2.1 Vigenère Cipher

The Vigenère cipher is a simple form of polyalphabetic substitution. It uses 26 different cipher alphabets to encrypt a message. The Vigenère Cipher consists of several Caesar Shift Ciphers in sequence with different shift values. To encipher, a table of alphabets can be produced called the Vigenère square. It consists of the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet[2]. At different points in the encryption process the cipher uses a different alphabet from one of the rows. For example if the plaintext to be encrypted is ATTACKATDAWN The person sending the message chooses a key and repeats it until it matches the length of the plaintext, for example the keyword “LEMON”

LEMONLEMONLE

The first letter of the plaintext is enciphered using the alphabet in row L which is the first letter of the key. This is done by looking at the letter in row L and column A of the Vigenère square namely L which can be determined from Figure 2.1. Similarly for the second letter of the plaintext, the letter at row E and column T is X. The rest of the plaintext is enciphered in a similar fashion.

Plaintext: ATTACKATDAWN

Key: LEMONLEMONLE

Cipher LXFOPVEFRNHR

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 2.1. Vigenère square used for the encryption and decryption cipher.

Decryption is performed by finding the position of the cipher text letter in a row of the table and taking the label of the column in which it appears as the plain text. For example in row L the ciphertext L appears in column A which is taken as the first plaintext letter.

$$e_i = m_i + k_i \mod 26 \qquad \text{Equation (2.1)}$$

Unlike normal alphabetic substitution, the Vigenère cipher is immune to frequency analysis. For a long time the Vigenère cipher was consider unbreakable and was often referred to as *le chiffre indéchiffrable.* The cipher was eventually broken by deducing the length of the keyword used in the polyalphabetic substitution cipher. With the length of the keyword known the ciphertext can be lined up into n columns. Each column can then be treated as the ciphertext of a single substitutional cipher and can be broken using frequency analysis [2].

2.2.2 One time pad

The one time pad, also called the Vernam-cipher, is a crypto algorithm where plaintext is combined with a random key. It is based on the Vernam Cipher developed by Gilbert Vernam in 1917. In order to achieve secrecy the following must be obeyed. The key should be as long as the plaintext message, the key should be truly random, there should only be two copies of the key, one for the sender and one for the receiver, and finally the key should only be used once. When used properly it is mathematically impossible

to crack a message encrypted using the one time pad. This concept was first developed by Claude Shannon in his famous paper on information theory [3]. To implement the one-time pad, Alice the sender and Bob the receiver, must produce a huge number of random bits and share them secretly. When Alice has a message to send to Bob, she retrieves a number of random bits equal to the length of her message, and uses them to be the message's key. She can apply the exclusive-OR operation (XOR) to the key and the message to produce the encrypted message. The key must be exactly the same size as the message. The key must also consist of completely random bits that are kept secret from everyone except Alice and Bob. When Bob receives the message, he retrieves the same bits from his copy of the random bit collection. He must retrieve the same random bits in exactly the same order that Alice used them. Then Bob uses the sequence of random bits to decrypt the message. He applies the XOR operation to the message and the key to retrieve the plain text.

2.2.3 Symmetric-key cryptography

The previous examples used symmetric key cryptography which is an encryption processes in which Alice and Bob share the same secret key. For Alice to send a message m to Bob they must first agree on a secret key k. Alice encrypts her message m using an encryption algorithm E to obtain a ciphertext $c = E(k, m)$. She then sends it to Bob who decrypts his message using his decryption algorithm D to recover the plaintext $m = D(k, c)$. Symmetric-key cryptography has the problem of how Alice and Bob can agree on the shared key in a manner which is secure and efficient. Nevertheless, this was the type of encryption used until the discovery of public-key cryptography in 1976 [4].

2.2.4 Public Key Cryptography

Symmetric-key cryptography which has been described to date has a number of practical limitations. The requirement that communicating parties share a common key which is known to no one else is not a trivial problem. It requires sending the key in advance by a secure channel often by a private courier. The advent of public-key cryptography eliminated the need for a secure communication channel and allowed communications between two parties even if they were previously unknown to each other [5]. Whitfield Diffie and Martin Helman in their 1976 paper [5] suggested a new type of public key distribution which requires only one key to be exchanged. In general public key cryptography is an asymmetric scheme that uses a pair of keys for

encryption, a public key E which is used to encrypt data and a corresponding private key D for decryption. A user publishes their public key to the world while keeping the private key secret. Anyone with a copy of your public key can then encrypt information that only you can read. It is presently computationally infeasible to deduce the private key from the public key if long keys are used. Anyone who has a public key can encrypt information but only the person who has the corresponding private key can decrypt the information. The scheme uses invertible functions E_K for encryption and D_K for decryption with the properties that for every key K, E_K is the inverse of D_K and that it is computationally difficult to obtain D_K from E_K.

2.2.5 Diffie–Hellman key exchange

In Diffie's and Helman's 1976 paper they also outlined a key exchange method which became known as the Diffie-Helman key exchange [5]. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. The scheme is based on discrete algorithms which take the form of

$$a \equiv g^m \pmod{n} \qquad \text{Equation (2.2)}$$

The key exchange as follows

(Private data in red, public data in blue)

1. Alice and Bob agree to use a prime number p=19 and base g=3.
2. Alice chooses a secret integer ***a*=14**, then sends Bob A=g^a mod p
   - A=3^{14} mod 19
   - A=**4,782,969** mod 19
   - A=4
3. Bob chooses a secret integer ***b*=26**, then sends Alice B=g^b mod p
   - B=3^{26} mod 19
   - B=**2,541,865,828,329** mod 19
   - B=6
4. Alice computes **s**=B^a mod p
   - **s**=6^{14} mod 19
     - **s=78,364,164,096** mod 19
   - **s=5**
5. Bob computes **s**=A^b mod p
   - **s**=4^{26} mod 19
   - **s=4,503,599,627,370,496** mod 19
   - **s=5**

6. Alice and Bob now share a secret: **s=5**. This is because **14×26** is the same as **26×14**. So somebody who had known both these private integers might also have calculated s as follows:
   - **s**=$3^{14\times26}$ mod 19
   - **s**=$3^{26\times14}$ mod 19
   - **s**=3^{364} mod 19
   - **s=52,226,895,197,709,578,372,156,471,421,169,310,383,980,817,485,079,062,358,448,435,612,040,315,502,855,394,952,348,837,866,966,144,815,836,290,966,448,962,341,841,264,961,544,065,279,388,544,410,108,981,718,679,226,404,541,792,809** mod 19
   - **s=5**

The Diffie-Hellman key exchange is vulnerable to the man-in-the-middle attack as the exchange protocol does not authenticate the participants.

2.2.6 RSA

The RSA algorithm for public key distribution was described by Ron Rivest, Adi Shamir and Leonard Adleman in 1978 [6]. RSA is an encryption method in which publically revealing the encryption key does not reveal any information about the decryption key. The two main important aspects of the encryption method they developed are

1: A secure means is not necessary to transmit keys since a message can be enciphered using an encryption key publically revealed by the intended recipient. Only he can decipher the message since only he knows the corresponding decryption key.

2: A message can be signed using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged.

A message is encrypted by representing it as a number M, raising it to the power e which has been publically revealed and then taking the remainder when the result is divided by n which is the production of two large secret prime numbers p and q. Decryption follows in a similar fashion where the secret power d is used such that $e \cdot d \equiv 1 \bmod (p-1)(q-1)$. The secrecy of the system relies on the difficulty of factoring the published divisor. Whereas the Diffie-Helman is a key exchange algorithm, RSA is an encryption/signing algorithm.

2.2.7 Problems with classical cryptography

Since the advent of public key cryptography the RSA encryption algorithm has proved hugely successfully for encrypting sensitive data used all around the globe by governments, militaries and the financial sector. However this security is based on the complexity of prime factorisation and the huge time required to reverse certain one-way functions with even the most powerful supercomputers. In 1991 RSA Laboratories setup the RSA Factoring Challenge with the goal of factorising larger numbers and cracking RSA keys. The largest number factorised was RSA-768 (768 bit number) but it took over two years to complete using hundreds of computers [7]. This demonstrates that security is not guaranteed infinitely as advances in factoring algorithms or computer technology may render current public-key cryptography systems insecure. One possibility is that with the invention of a quantum computer, in which a single bit can be represented by a quantum superposition of a binary 1 and 0, could dramatically decrease the time required for prime factorisation. Shor's algorithm[8], which runs on a quantum computer, runs exponentially faster than the best classical factorising algorithm. A demonstration of this was first reported in 2001 by a group from IBM who used seven spin ½ nuclei in a molecule to find the prime factors of 15, 3 and 5 [9]. Although the number factored is quite small, it nevertheless demonstrates the possibilities. At first it appeared a quantum computer could spell the end of modern cryptography but it was soon realised that the properties of quantum mechanics which gives a quantum computer its huge potential could also be used in a new idea of quantum cryptography. This new idea relied on the fundamental laws of quantum mechanics for its security and not on the difficulty of prime factorisation.

2.3 Quantum Cryptography

The concept of quantum cryptography was first proposed in the 1970's by Stephen Wiesner. Wiesner's paper called "Conjugate Coding" [10] proposed the notion of quantum bank notes which would be impossible to counterfeit by encoding a two state system in orthogonal and non-orthogonal basis sets. The quantum bank notes could contain a series of light traps, each of which would be filled with randomly polarised photons. The polarisation can only be read out and restored by the bank who knows the exact sequence of polarised filters needed to read the serial. Then in October 1979 a chance meeting on a beach in Puerto Rico between Charles Bennett and Gilles Brassard laid the groundwork for the new field of quantum cryptography. They combined ideas from Wiesner's coding scheme with new concepts which were developing in public key

cryptography [11]. The first quantum cryptography key protocol was proposed by Bennett and Brassard in 1984 and is referred to as the BB84 protocol [12]. The security of the protocol is guaranteed by the basic principles of quantum mechanics, namely, it is impossible to make a measurement without perturbing a quantum system, one cannot determine simultaneously the position and momentum of a particle with absolute certainly and finally, it not possible to duplicate an unknown quantum state, referred to as the no cloning theorem. The no cloning theory is a direct consequence of quantum mechanics which forbids the creation of identical copies of an arbitrary quantum state and was described by Wooters *et al.* in 1982 [13]. The ability to clone a quantum state would be in violation of the Heisenberg Uncertainty Principle [14]. The consequences of this is that eavesdropper is not able to intercept qubits sent from Alice and make a perfect copy of them and then resend the original to Bob, which prevents her from measuring the qubits having listened into the public discussion between Alice and Bob about basis set reconciliation.

The schematic of a general QKD system is shown in Figure 2.2. Alice sends her quantum bits (qubits) to Bob over the quantum channel. A public classical authenticated channel is used later for post-processing of the data [15]. This authentication can be provided by classical digital signatures or quantum digital signatures. It is assumed that an eavesdropper Eve can listen in on the quantum channel to gain information on the key.

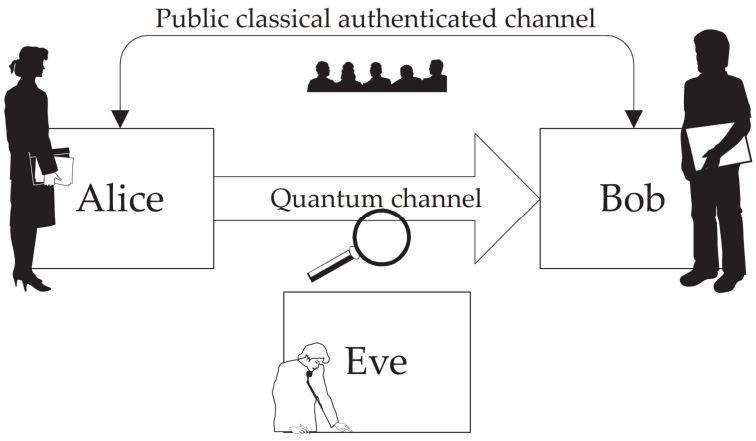

Figure 2.2. The QKD system consists of a quantum channel in which Alice sends her single-photons to Bob. A public classical authenticated channel is used after transmission for reconciliation and error correction. It is assumed that an eavesdropper can listen into the quantum channel [15].

2.3.1 BB84 protocol using the non-orthogonality of quantum states

The BB84 protocol for distributing quantum keys derives part of its security by encoding information on two mutually non-orthogonal states of a photon. If light is polarised at a particular angle α and is sent through a polariser orientated at an angle β then the transmitted photons are transmitted with probability $\cos^2(\alpha-\beta)$ and those that do not make it through with probability $\sin^2(\alpha-\beta)$. The photons only behave deterministically when the two axes are parallel where the probability of transmission is 1 or when the axes are perpendicular, where the probability of transmission is 0. When the axis are not perpendicular so that some of the photons are transmitted one might hope to learn additional information about α by measuring the transmitted photons again with a polariser orientated at some third angle, by this is fruitless because the transmitted photons in passing through β polariser emerge with exactly a polarisation β having lost all information about their previous polarisation α. The BB84 protocol uses two basis sets for encoding a binary 0 or 1 as shown in Figure 2.3. Vertical and horizontal polarisation states (linear basis) are used in one basis while left and right circular states are used in the other (circular basis). In each basis set the states are orthogonal to each other while states from different basis are non-orthogonal. The use of these non-orthogonal quantum states for representing a binary 1 or 0 is one of the underlying principles which guarantees the security of QKD. Only when Alice and Bob use the same basis set for encoding does Bob obtain an unambiguous result on his detectors. This can be seen in Figure 2.4 and Figure 2.5.

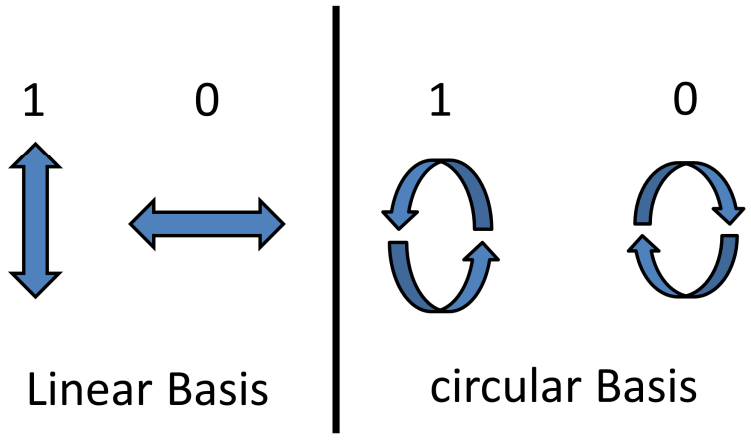

Figure 2.3.Two basis set required for BB84. The states for encoding a binary 1 and 0 are orthogonal in a given basis set but are non-orthogonal in different basis sets. Here 1 and 0 are represented by horizontal and vertical polarised light in one basis and left and right circular in the other.

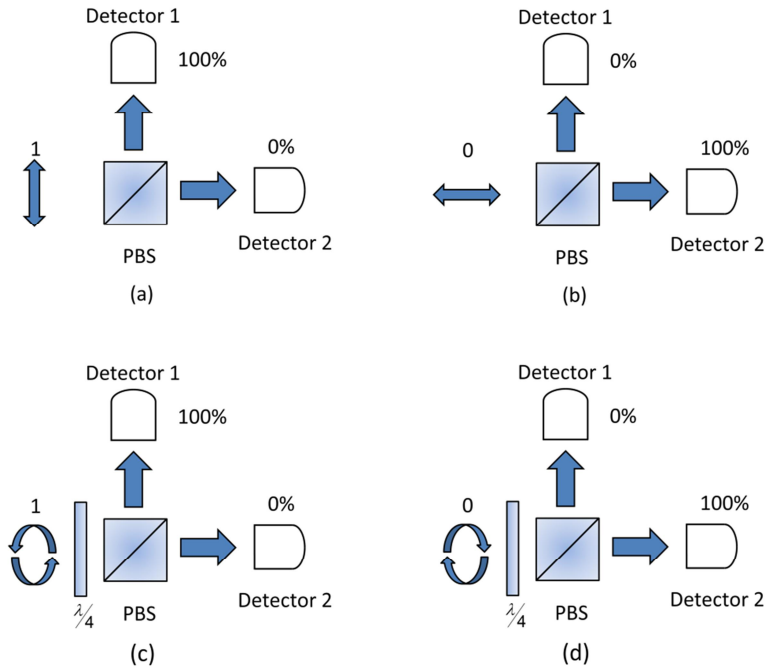

Figure 2.4. Demonstration of an unambiguous measurement by Bob with a polarisation beam splitter (PBS) using polarisation encoding. Polarisation axis are aligned that vertical polarised light is 100% reflected at PBS in (a) and horizontal polarised light is 100% transmitted as in (b). In the case of right (c) and left circular (d) polarisation unambiguous measurements is obtained on transmission through a quarter wave plate $(\lambda/4)$.

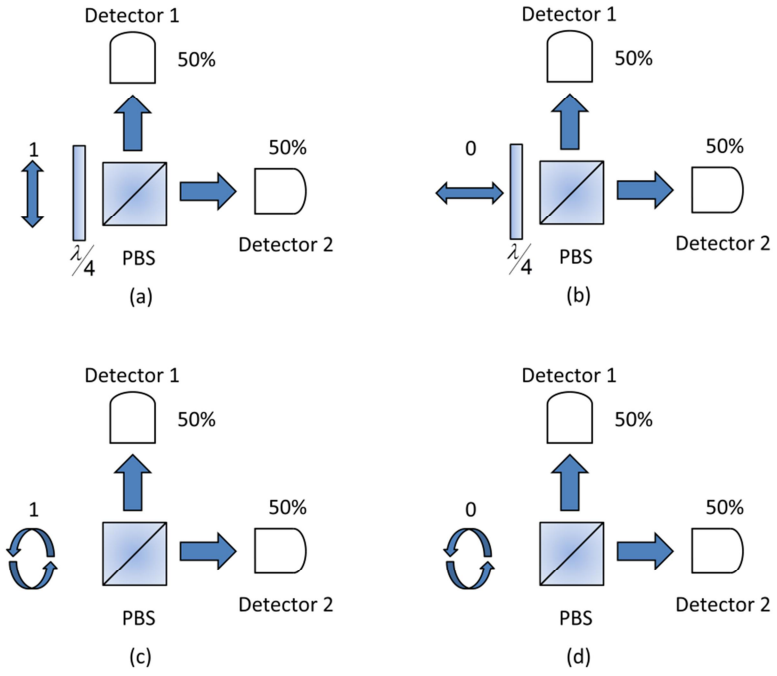

Figure 2.5. Demonstration of an ambiguous measurement by Bob using a PBS using polarisation encoding. For each case (a), (b), (c) and (d) detector 1 and detector 0 can fire with 50% probability.

The BB84 protocol proceeds as follows (Table 2.2): Alice the sender chooses a random bit string and a random sequence of polarisation bases either linear or circular. She then sends to Bob a train of photons each representing one bit of the string in the basis chosen for that bit position, a horizontal or right circular polarisation representing a binary zero and a vertical or left circular polarisation representing a binary 1. As Bob receives the photons he decides randomly for each photon whether to measure the photons rectilinear polarisation or its circular polarisation. All the information is lost when he attempts to measure the rectilinear polarisation of a photon with a circular polarisation and vice versa. Therefore Bob only obtains useful information from only half of the photons he detects, those for which he guessed the correct polarisation basis. The information that Bob receives is also affected by the fact that some of the photons are lost in the transmission or would fail to be detected due to inefficient detectors.

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random basis set selection	+	+	○	+	○	○	○	+
Photon polarisation Alice sends	↑	→	↻	↑	↻	↻	↻	→
Bobs random measuring basis	+	○	○	○	+	○	+	+
Photon polarisation Bob Measures	↑	↻	↻	↻	→	↻	→	→
Public Discussion of basis	✓	✗	✓	✗	✗	✓	✗	✓
Shared Secret Key	0		1			0		1

Table 2.2. Progression of the BB84 protocol for quantum key distribution. The linear polarisation basis set is denoted by + and the circular basis set is denoted by ○. The coloured ticks indicate if Alice and Bob choose compatible basis sets while the greyed boxes indicate bits which have been discarded after basis set reconciliation because Bob measured in the wrong basis set.

Alice then publically reveals to Bob in which basis set a particular photon was sent but not its bit value. They then perform basis set reconciliation in which they agree to disregard those events in which incompatible basis sets were used, to create a sifted key.

If the basis set choice was completely random they discard 50% of the original bit string. Alice and Bob can test for the presence of an eavesdropper by publicly comparing some of the bits on which they think they should agree and calculate a figure of merit called the quantum bit error rate (QBER), which is the fraction of wrongly encoded bits divided by the total number sent. The bit position used in this comparison should be a random subset of the correctly received bits and are discarded for final key generation. If all the comparisons agree Alice and Bob can conclude that the quantum transmission has been free of significant eavesdropping and that the remaining bits can be safely used as a one-time pad for subsequent secure communication over the public channel. The preceding assumes the communication system is of free of errors. These errors can arise from optical imperfections in the transmitter/receiver stations, transmission losses, detector imperfections and eavesdropping. To reduce these errors to a minimum, error correction and privacy amplification steps are then performed which are discussed in section 2.5.2.

2.3.2 Phase encoding for QKD

The idea of phase encoding was first mooted by Bennett in 1992 [16]. State discrimination of phase encoded states can be performed using interferometers. Figure 2.6 shows a single balanced Mach-Zehnder interferometer for use in quantum cryptography.

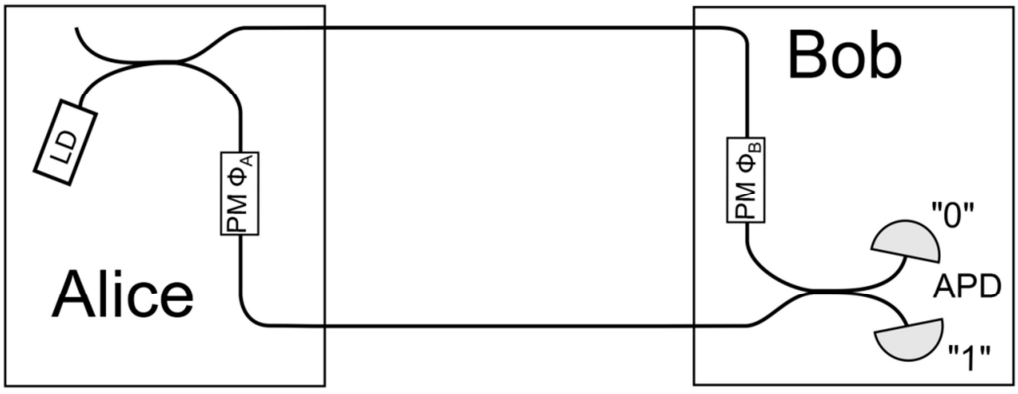

Figure 2.6. Schematic of a balanced Mach-Zehnder interferometer. Alice can apply her phase shift ϕ_A using her phase modulator (PM) and Bob makes his basis set choice with his phase modulator applying a random phase shift of ϕ_B [17].

When the path length difference between the arms is kept smaller than the coherence length of the source interference is observed. The intensity at the detector labelled 0 is given by

$$I_0 = I\cos^2\left(\frac{\phi_A - \phi_B + k\Delta L}{2}\right) \qquad \text{Equation (2.3)}$$

where $\phi_A - \phi_B$ is the phase difference between Alice's and Bob's phase modulator, I is the input intensity, k is the wavenumber and ΔL is the path length difference. When $\phi_A - \phi_B = \pi/2 + n\pi$, destructive interference is observed and when $\phi_A - \phi_B = n\pi$, constructive interference is observed (n is an integer value). For intermediate phase the light is split depending on the phase difference. This implementation can be used for quantum cryptography where single-photons are used. The interference observed can be considered as the equivalent of Young's slit experiment where the arms of the interferometer have replaced the slits [17].

In quantum cryptography Alice can apply one of 4 phase shifts to encode a bit value. Bob performs a basis set choice by randomly selecting a phase shift of 0 or π. When Alice's and Bob's phase choice differs by 0 or π Bob's detectors behave deterministically. However, if the phase difference is half integer of π each of Bob's detectors clicks with 50% probability. This can be seen more clearly in Table 2.3.

Alice		Bob		
Bit value	ϕ_A	ϕ_B	$\phi_A - \phi_B$	outcome
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$	?
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$	?
0	$\pi/2$	0	$\pi/2$	?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$	?
1	$3\pi/2$	$\pi/2$	π	1

Table 2.3. Shows the available phase encoding options available for Alice and Bob for implementing the BB84 protocol in phase. When the applied phase difference between Alice and Bob is 0 or π Bob's detectors behave deterministically and he receives a 1 or 0. When the applied phase difference between Alice and Bob is $3\pi/2$ or $\pi/2$ Bob's detector clicks with 50% probability which gives an ambiguous result denoted by "?".

The schematic just described is impractical to implement over long distances as maintaining the path length difference becomes impossible due to environmental fluctuations. This problem can be overcome by the use of unbalanced Mach-Zehnder interferometers connected in series by a single fibre shown in Figure 2.7. Now Alice and Bob only have to keep their path length stabilised over a much shorter distance. To maintain the path length difference and to reduce polarisation evolution of the state it is necessary to keep the temperature constant and to eliminate stress in the fibre. This setup was first demonstrated by Townsend, Rarity and Tapster in 1993 over a 10 km quantum channel [18]. The approach also required alignment of the polarisation state of the photons at Bob and required corrections in the path lengths in the arms of the interferometer.

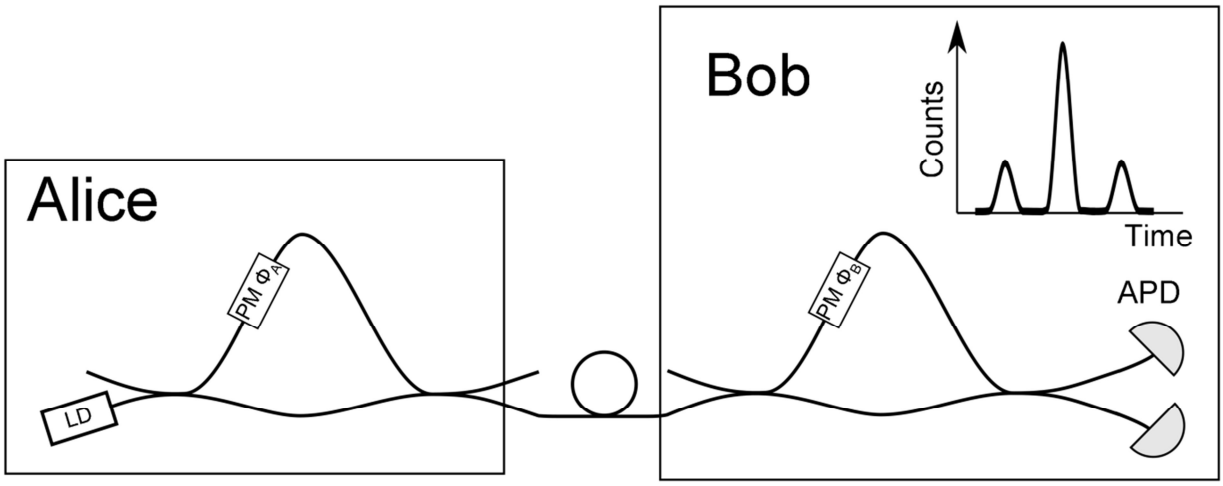

Figure 2.7. Schematic of the unbalanced Mach-Zehnder interferometer approach for QKD. If Bob monitors his count rate as a function of time three peaks are observed. The pulse left and right of the central peak correspond to non-interfering photons that have taken the short path in Alice and Bob or the long path in Alice and Bob. The central pulse which undergoes interference is due to photons which have taken the short path in Alice and the long in Bob and vice versa[17].

2.4 Other QKD protocols and experimental implementations

2.4.1 B92

In 1992 Bennett realised that only two states were required for QKD only if the states are not mutually orthogonal to each other [16]. The protocol relied on the fact that non-orthogonal states cannot be unambiguously distinguished with 100% success probability. However in 1987 Ivanoic proved that unambiguous states discrimination is

possible but with the drawback of additional losses [19] a situation shown experimentally by Huttner *et al.* in 1996 [20]. For the B92 protocol Alice sends a random binary sequence of non-orthogonal states $|\phi\rangle$ and $|\varphi\rangle$ to represent the binary bit 1 and 0 as shown in Figure 2.8. Let the projection operators $P_0 = 1 - |\phi\rangle\langle\phi|$ and $P_1 = 1 - |\varphi\rangle\langle\varphi|$ have the property that P_0 acting on $|\varphi\rangle$ annihilates the state but a deterministic result is obtained with probability $1 - |\langle\phi|\varphi\rangle|^2 / 2 > 0$ when it acts on $|\varphi\rangle$. Bob randomly chooses to make a measurement of P_0 or P_1. He then publically announces to Alice only when his measurements had a positive result and they both discard all other cases. In the absence of an Eavesdropper, Bob achieves unambiguous discrimination with a probability given by

$$1 - |\langle\phi|\varphi\rangle|^2 / 2 \qquad \text{Equation (2.4)}$$

The B92 protocol has the advantage of not requiring two basis sets like in BB84 but does offer a potential eavesdropper the opportunity to replace the quantum channel with a lossless one in which the presence of an Eavesdropper would go unnoticed.

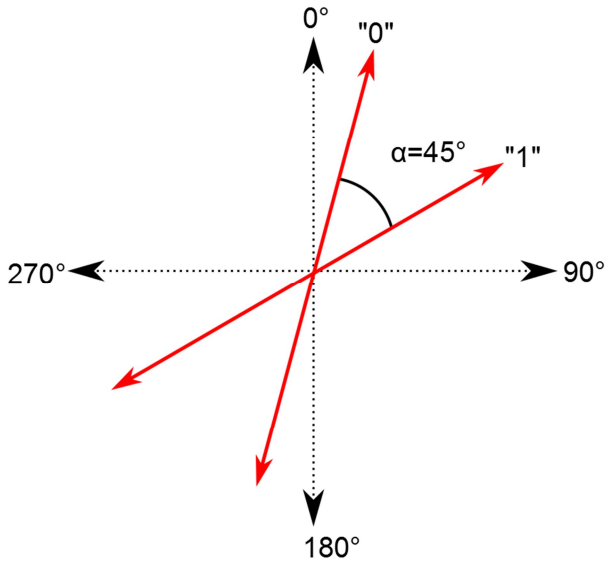

Figure 2.8. Two orthogonal states required for B92. When the angle α is 45° Bob's success probability of correctly determining the state is given by 1-cos45=0.2928.

2.4.2 Distributed phase reference protocols

2.4.2.1 Coherent one-way time coding

The BB84 protocol proposed by Bennett and Brassard uses two orthogonal basis sets *X* and *Y* for encoding. It is also possible to use a third basis $\{|1\rangle|0\rangle, |0\rangle|1\rangle\}$ which when implemented involves measuring the time-of-arrival of photons and is insensitive to optical errors. A schematic of the method is shown in Figure 2.9. Alice uses her laser

to produce a pulse with mean photon number μ for encoding 0 or 1 and "vacuum" pulses by using her intensity modulator. The sequences of 1 and 0 occur with probability $(1-f)/2$ and the vacuum pulses occur with probability $f \ll 1$. After transmission of the sates Bob reveals which bits he obtained on detector D_B and detector D_{M2}. Alice then tells Bob the bits he must remove from his raw key which are due to the detection of decoy sequences. Alice then analyses the detection event in D_{2M} to estimate the break of coherence by examining visibility V_{1-0} and V_d which are associated with 1-0 bit sequences and decoy sequences respectively. Since equally spaced pulses are produced, the coherence of both decoy and 1-0 bit sequences can be checked by a single interferometer. The scheme has the added benefit that it is able to detect the photon number splitting attack as Eve cannot count the number of photons in any finite number of pulses without introducing errors [21].

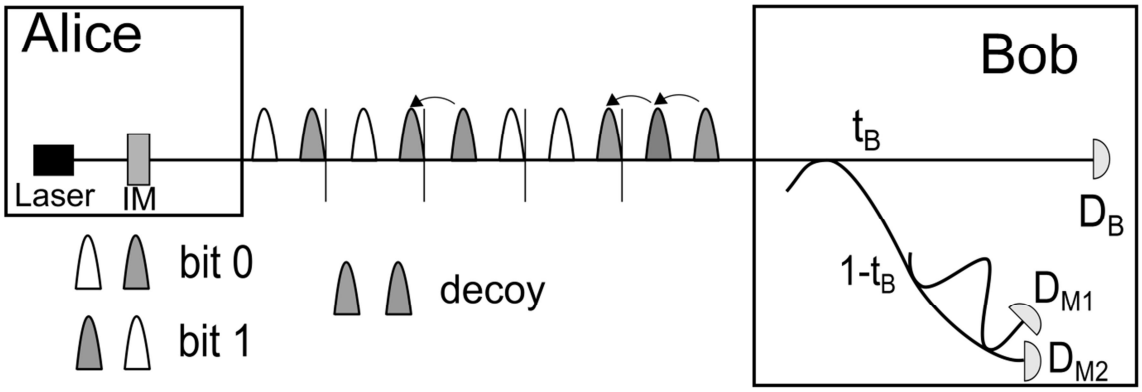

Figure 2.9. Schematic of the quantum channel for implementing coherent one-way time-coding. The pulse are sent to Bob and are split at an unequal beamsplitter with transmission $t_B \ll 1$. The interferometer is used to check the quantum coherence [21].*(IM intensity modulator)*

2.4.2.2 Differential Phase sift protocol

Differential phase shift (DFS) QKD uses a weak coherent pulse train of the form $|\psi\rangle = |e^{i\psi_{k-1}}\sqrt{u}\rangle |e^{i\psi_k}\sqrt{u}\rangle |e^{i\psi_k}\sqrt{u}\rangle \ldots$, where ψ can be 0 or π [17]. Alice sends the coherent pulse train to Bob with an average intensity less than one photon per pulse. Each pulse is randomly modulated by 0 or π. Bob's receiver consists of a Mach-Zehnder interferometer whose delay is chosen to be the same as the pulse interval as shown in Figure 2.10. This causes neighbouring pulses to interfere with each other. The bits are encoded using the difference between two successive phases. Bob detects a

bit 0 if $e^{i\psi_k} = e^{i\psi_{k+1}}$ or 1 if $e^{i\psi_k} \neq e^{i\psi_{k+1}}$. The key is generated after transmission by Bob revealing to Alice the time slots in which his detector clicked. From Bob's information and Alice's phase encoding information Alice can determine which of Bob's detector clicked. Each detector is designated for a binary 1 or 0. No photons are thrown away during the basis matching as bit information is not disclosed. General security is given by the mean photon number being less than one. If Eve tries to tap part of the signal since photon events are rare there is a small probability of Eve and Bob detecting a photon from identical pulses ensuring information leakage is small [17].

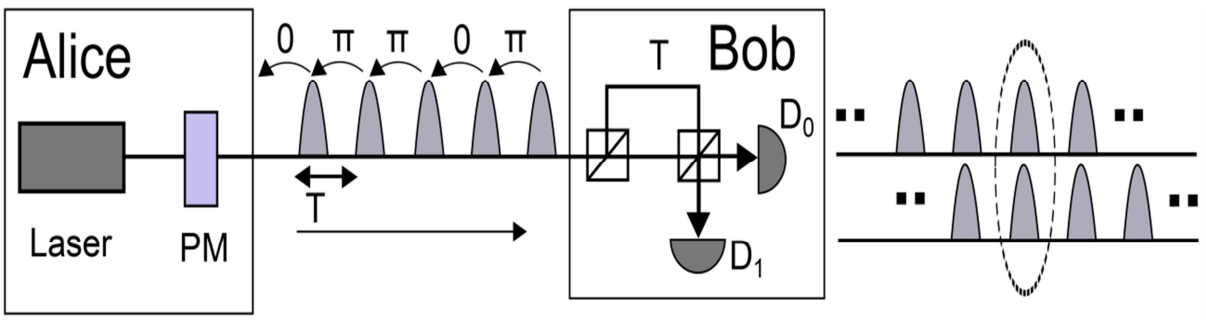

Figure 2.10. Schematic of the differential phase shift for QKD. The delay in the interferometer is chosen that neighbouring pulse interfere with each other [22].(Pm is the phase modulator)

2.4.3 Continuous variable QKD

To combat the necessity of using a single-photon state in the original vision of the BB84 protocol which is difficult to produce and detect, continuous variable (CV) protocols in QKD using Gaussian modulated coherent states and homodyne detection were proposed by Grangier in 2002 [23]. Homodyne detection techniques which can make good use of high speed detectors with near unit efficiency. A coherent state $|\alpha\rangle$, in Dirac notation, is the quantum mechanical equivalent of a classical electromagnetic wave and can be written as

$$\alpha = X_1 + iX_2 \qquad \text{Equation (2.5)}$$

where X_1 and X_2 are dimensionless quadratures of the field. When written as $\alpha = |\alpha| e^{i\phi}$ it can be represented on a phasor diagram (Figure 2.11) where $|\alpha| = \sqrt{X_1^2 + X_2^2}$ is the amplitude. A coherent state is a minimum uncertainty state which means that

$$\Delta X_1 = \Delta X_2 = \frac{1}{2} \qquad \text{Equation (2.6)}$$

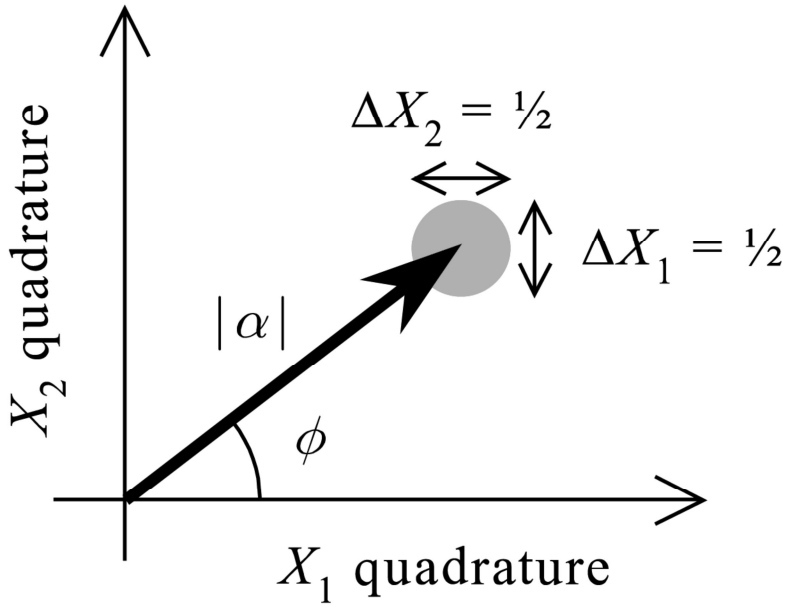

Figure 2.11. Phasor representation of a coherent state. The length of the phasor is given by $|\alpha|$ and ϕ is the optical phase. The quantum uncertainty is represented by the grey circle of diameter $1/2$

The CV QKD protocol proposed by Grangier *et al.* was based on a similar idea in the BB84-type protocol and uses many non-orthogonal bases represented by slight modulations of different quadrature amplitudes. The security of the protocol uses the fact that coherent states are non-orthogonal which results in an ambiguity in trying to determine the states. To ensure the sufficient overlap between all signal states, the scheme operates at a low light level. The CV QKD protocol proceeds as follows: Alice generates coherent states of the form $\alpha = |\alpha| e^{i\theta} = (X_1 + iX_2)$ with Gaussian distributed quadratures and sends them to Bob via a quantum channel along with a strong phase reference or strong local oscillator. In Bob's system the local oscillator is randomly shifted by either 0 or π. Bob then randomly measures the X_1 or X_2 quadrature by homodyne detection methods by making the signal interfere with the local oscillator. The intensity on the homodyne detection system is directly proportional to the rotated quadrature of the signal. Bob then publically reveals to Alice in which quadrature he measured in order for Alice to discard irreverent data [23]. Binary 1 and 0 are designated depending on the sign of the signal from the homodyne detector. Figure 2.12 shows a schematic of a CV QKD scheme used in the SECOQC QKD network.

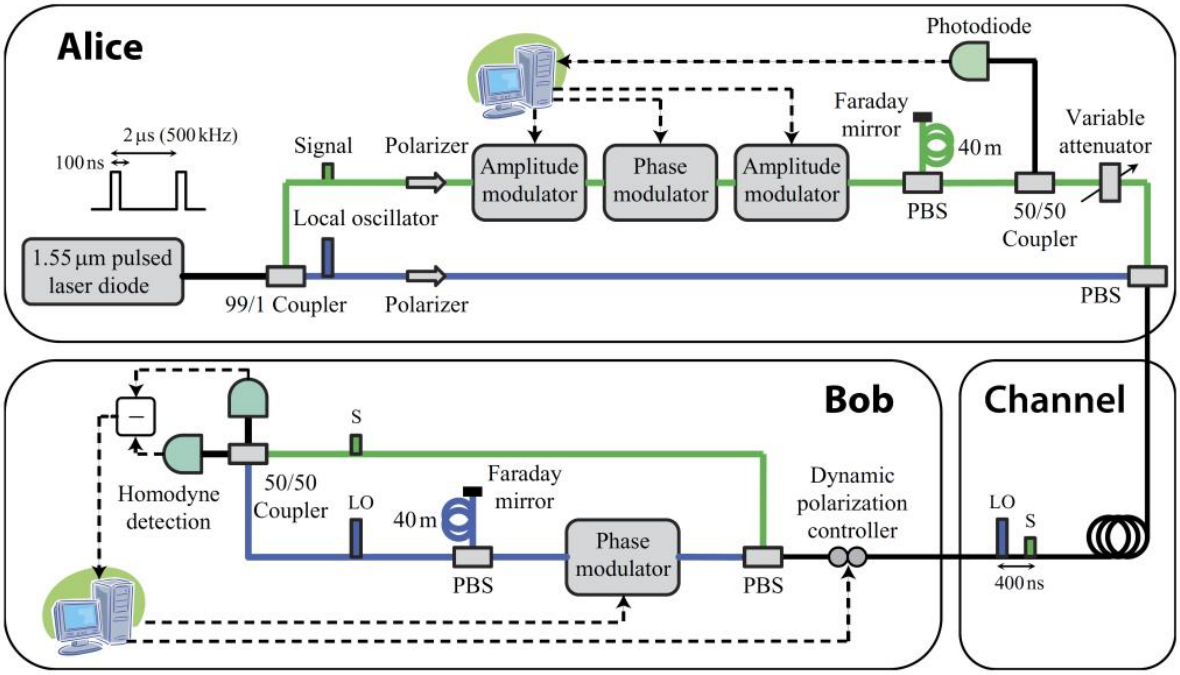

Figure 2.12. Schematic of a continuous variable (CV) QKD system used in the SECOQC QKD network [24].

2.4.3.1 Entanglement, EPR paradox and non-locality

In the 1930's there was fierce debate relating to the interpretation of quantum mechanics. Scientists like Albert Einstein were deeply unhappy with the Copenhagen interpretation of quantum mechanics proposed by Neils Bohr where physical properties like spin and polarisation seemed to depend on the measurement process itself. In 1935 the famous paper now commonly referred to as EPR was published by Einstein along with Podolsky and Rosen and was an attempt to prove the 'incompleteness' of quantum mechanics [25]. Einstein was in favour of using so called hidden variables to provide a complete descriptive account of all observable behaviour and eliminate the indeterminism of quantum mechanics. The EPR thought experiment consisted of two particles A and B who are allowed to interact with each other briefly, thereby becoming entangled, and are then separated. One of the simplest systems in which entanglement occurs is for two spin ½ particles.

$$\left|\varphi_{\text{sin glet}}\right\rangle = 1/\sqrt{2}\left(\left|0,1\right\rangle - \left|1,0\right\rangle\right) \qquad \text{Equation (2.7)}$$

for particle A and B with 0 and 1 the notation for spin 'up' and spin 'down'. This singlet state has zero total angular momentum and it arises often in atomic physics. In the ground level of hydrogen the electron and nuclear spins are found in this state. The entanglement is the result of the hyperfine coupling between the electron and the nuclear spin. A system of particles is said to be entangled if its wave function cannot be

factorised into a product of the wave function of the individual particles. After the particles have been entangled the uncertainty principle prevents the exact measurement at a given instance of both the position and momentum of either particle however it does allow the exact and simultaneous measurement of the total momentum of A and B and the relative distance between them. The idea in is then to leave particle B undisturbed by not making any direct observation of it. No matter how far apart A and B are quantum mechanics allows a measurement of the momentum of A revealing information about the exact momentum of B, with B being not being disturbed in the measurement process. In effect when the momentum of A is measured exactly, it indirectly but simultaneously allows the exact momentum of B to be determined. Einstein referred to this process as "spooky-action-at-a-distance". He argued that locality prevented the possibility of an event in a certain region of space to influence another event simultaneously elsewhere when separated by even large distances. This idea of locality was the key assumption in the EPR argument in which simultaneously action at a distance does not exist. In the Copenhagen approach the measurement of the state of one entangled particle instantaneously determines the result of the other, an idea referred to as nonlocality. Then in 1964 John Bell published work that showed that results predicted by quantum mechanics, like the EPR thought experiment, could not be explained by any theory which preserves locality [26]. Bell derived an inequality which is always obeyed if the local hidden variables of the microscopic world are correct whereas quantum mechanics predicts violations of his so called Bell's inequality. These violations were subsequently experimentally found by experiments performed by Aspect *et al.* [27] in which they looked at linear polarisation correlations of pairs of photons emitted in a radiative cascade of calcium. Bell's inequality can be explained by considering Aspect *et al.*'s experiment. After a source emits pairs of spin ½ particles, correlation measurements of their spin components can be carried out along arbitrary directions $\vec{a}$ and $\vec{b}$. For each measurement yields two results. For a photon measured along $\vec{a}$ yields +1 if the polarisation is found parallel to $\vec{a}$ and -1 if the polarisation is found perpendicular. Quantum mechanics also predicts measurement outcomes between these two values. The term $P_{\pm\pm}\left(\vec{a},\vec{b}\right)$ describes the probabilities of obtaining the result ±1 along $\vec{a}$ and ±1 along $\vec{b}$. The quantity given by

$$E\left(\vec{a},\vec{b}\right) = p_{++}\left(\vec{a},\vec{b}\right) + p_{--}\left(\vec{a},\vec{b}\right) - p_{+-}\left(\vec{a},\vec{b}\right) - p_{-+}\left(\vec{a},\vec{b}\right) \quad \text{Equation (2.8)}$$

expresses the correlation coefficient of the measurement on the two particles. Bell examined theories explaining these correlations as a result of common properties of both particles of the same pair. When he added the assumption of locality he was able to demonstrate that these correlations are constrained by certain inequalities that are not always obeyed by the predictions of quantum mechanics. These theories lead to the generalised Bell's inequality given by

$$-2 \le S \le 2 \qquad \text{Equation (2.9)}$$

where

$$S = E\left(\vec{a},\vec{b}\right) - E\left(\vec{a},\vec{b'}\right) + E\left(\vec{a'},\vec{b}\right) + E\left(\vec{a'},\vec{b'}\right) \qquad \text{Equation (2.10)}$$

This involves measurements in four various orientations along $\vec{a}, \vec{a'}, \vec{b}$ and $\vec{b'}$. For suitable sets of orientations, quantum mechanics predicts that S can reach values of $\pm 2\sqrt{2}$ which is in violation of Equation (2.9) and shows that quantum mechanics is not compatible with a theory which preserves local variables.

2.4.3.2 E91 protocol

In 1991 Ekert [28] devised a QKD scheme using the Einstein-Podolsky-Rosen (EPR) thought experiment [25] and the use of Bell's inequality to test for security. Bell's inequality predicts correlations which are stronger than any classical counterpart [26]. In the QKD scheme (Figure 2.13), a sources emits two entangled qubits with a state given by

$$\left|\Phi^{+}\right\rangle_{12} = \frac{1}{\sqrt{2}}\left(\left|H_1\right\rangle\left|H_2\right\rangle + \left|V_1\right\rangle\left|V_2\right\rangle\right) \qquad \text{Equation (2.11)}$$

and are separated, one being sent to Alice and one sent to Bob. They perform polarisation measurements using a polarisation beam splitter and two single-photon detectors. Alice will obtain 1 if detector 1 fires and a 0 if detector 2 fires. If Bob chooses the same basis set he will always obtain the same result as Alice. From ideas put forward by EPR, Alice is able to predict with certainty what Bob's result will be. The principle of locality means that no physical signal can go instantly from Alice's detection system to Bob's which means that Bob's measurement results depends only on his detection system and the properties of his qubit. Bell investigated the possible correlations for the case when Alice and Bob chose detection bases with arbitrary oblique angles α, β and γ. The quantity S given in Bell's inequality is composed of the correlation coefficients when Alice and Bob uses analyser of different orientations

and quantum mechanics requires that $S = -2\sqrt{2}$. After transmission has taken place Alice and Bob publically announce the orientation of the analyser for each particular measurement. For the case where they used different orientation of analysers Alice and Bob publically reveal the result they obtained which allows them to calculate S which should give a result of $S = -2\sqrt{2}$. In the case of measurements where they choose the same polarisation orientation the measurements are anti-correlated and converted into the key. If an eavesdropper has been present the entanglement between Alice's and Bob's state will be broken which results in a value of S deviating from the expect value predicted by quantum mechanics. Key generation should be halted if $-2\sqrt{2} \le S \le 2\sqrt{2}$ which implies the presence of an Eavesdropper [29].

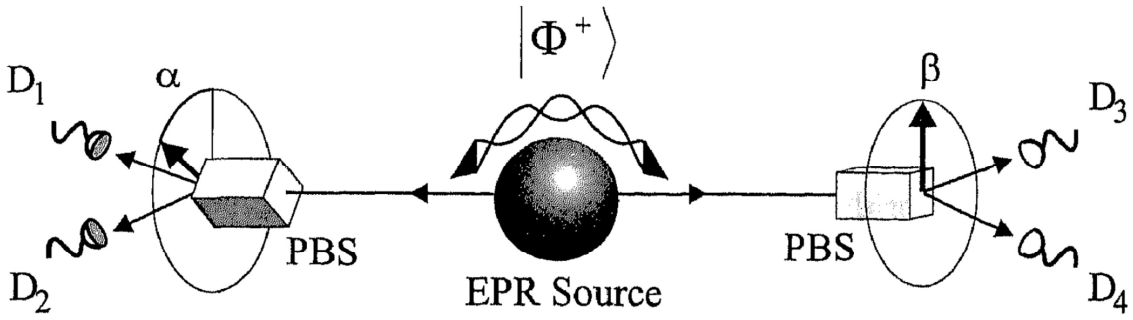

Figure 2.13. Correlation measurements between Alice's and Bob's detection events for different choices for the detection bases indicated by the angles α and β for the orientation of the polarisation beam splitter (PBS) lead to violation of Bell's inequality [29].

2.4.4 Quantum dense encoding

In 2000 a protocol for QKD based on a higher dimensional system than the two level quantum system traditionally used in quantum cryptography was proposed. The protocol is based on using four orthogonal states in two different basis sets and offers an increase in the key generation rate since every photon carries more information. Similarly as in the case of the BB84 protocol Alice first randomly selects one of the two basis sets to encode the information and then unlike in BB84 she then selects from one of the four states. With the 4-dimensional case, each of the states occurs with probability 1/8. The first basis set can be given by the following

$$|\psi_\alpha\rangle, |\psi_\beta\rangle, |\psi_\gamma\rangle, |\psi_\delta\rangle$$

With each of the states being orthogonal to each other, $\left|\langle\psi_i|\psi_j\rangle\right| = \delta_{ij}$. The second basis set ϕ must have the property that $\left|\langle\psi_i|\phi_j\rangle\right| = \frac{1}{2}$ to ensure the protocol is symmetric. These states take the form

$$|\phi_\alpha\rangle = \tfrac{1}{2}\left(|\psi_\alpha\rangle + |\psi_\beta\rangle + |\psi_\gamma\rangle + |\psi_\delta\rangle\right),$$
$$|\phi_\beta\rangle = \tfrac{1}{2}\left(|\psi_\alpha\rangle - |\psi_\beta\rangle + |\psi_\gamma\rangle - |\psi_\delta\rangle\right),$$
$$|\phi_\gamma\rangle = \tfrac{1}{2}\left(|\psi_\alpha\rangle - |\psi_\beta\rangle - |\psi_\gamma\rangle + |\psi_\delta\rangle\right),$$
$$|\phi_\delta\rangle = \tfrac{1}{2}\left(|\psi_\alpha\rangle + |\psi_\beta\rangle + |\psi_\gamma\rangle - |\psi_\delta\rangle\right)$$

each with the property that $\left|\langle\phi_i|\phi_j\rangle\right| = \delta_{ij}$. Every time Bob receives a states he must randomly choose to measure in the ϕ or ψ basis set (time and energy basis set).

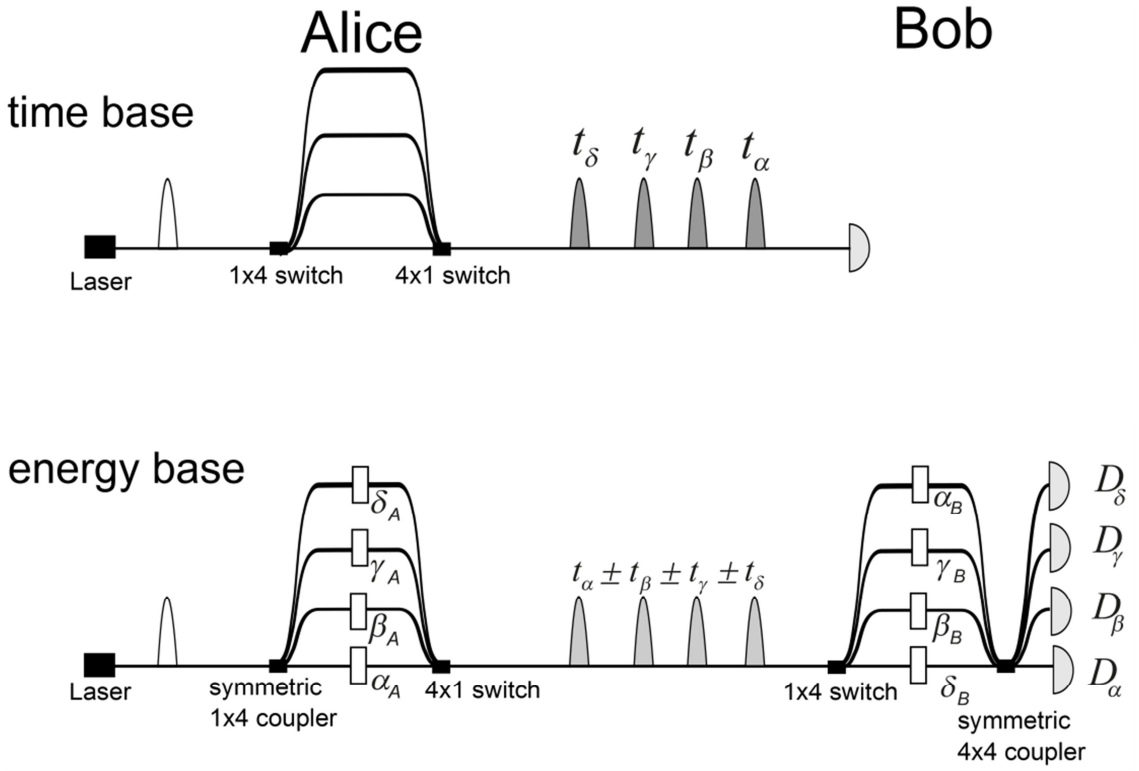

Figure 2.14. Schematic for four-letter quantum key distribution [30].

This can be achieved experimentally by Alice routing her photons into one of 4 time delays shown in the upper diagram in Figure 2.14. Then using another optical switch a photon with a desired delay $\left(t_\alpha, t_\beta, t_\gamma, t_\delta\right)$ can be emitted to Bob. For Bob to distinguish each of the 4 states in the basis all he is required to do is measure the arrival time of the pulse with respect to t_0, the initial time. In order for Alice to produce a superposition of the four emission times with appropriate phase differences, a 1×4 optical coupler shown in the lower diagram in Figure 2.14 is used. The states $|\phi_\alpha\rangle, |\phi_\beta\rangle, |\phi_\gamma\rangle, |\phi_\delta\rangle$ can be

created by randomly applying a phase of $\alpha_A, \beta_A, \gamma_A, \delta_A$. For Bob to distinguish the states in this basis set he takes the pulse arriving at time $t_\alpha, t_\beta, t_\gamma, t_\delta$ and recombines them to achieve constructive or destructive interference on a particular output [30].

2.4.5 "Plug-and-play" system

To overcome some of the difficulties posed by the unbalanced Mach-Zehnder approach described in section 2.3.2, in 1997 a system was designed and built using phase encoding in which optical and mechanical fluctuations are compensated for using a system called "*plug-and-play*" [31]. The system made use of the fact that when a light pulse travels through an optical fibre and is reflected by a Faraday mirror the output polarisation state is orthogonal to the input regardless of fluctuations in the birefringence due to environmental effects. A schematic is shown in Figure 2.15.

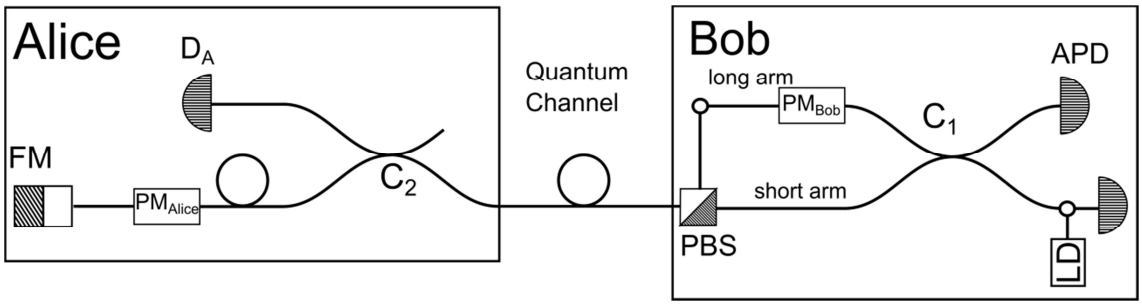

Figure 2.15. Schematic of the "plug-and-play" system. The time multiplexed arrangement ensures that inferring pulses travel through the same optical path which removes the need for path length control. The additional of Faraday mirrors (FM) ensures that the system is immune to random fluctuations in birefringence due to environmental effects [31]. LD is a laser diode, APD is an avalanche photodiode, D_A is a photodiode and C_1 and C_2 are optical couplers.

A laser pulse is injected into the system via an optical coupler. At coupler C_1 it is split into two parts, P1 and P2. P1 propagates through the short arm in Bob and its polarisation is arranged that it is transmitted at the polarisation beam splitter (PBS) and is sent to Alice. P2 takes the long arm in Bob and its polarisation is such that it is reflected at the PBS but no phase shifted is added. The pulse P2 is then sent to Alice delayed with respect to P1. At Alice P1 is diverted by coupler C_2 where it is detected by a classical detector D_A to provide a timing reference. The light which is not diverted travels through an attenuator and an optical delay line. The light is then reflected by a Faraday mirror which rotates the polarisation by 45º on a single pass. A Faraday mirror is a non-reciprocal optical device which means that the direction of rotation of the polarisation is independent of the light propagation direction. This is used to eliminate

the time evolving birefringence effects which would randomly change the state of polarisation of the light. The pulse P2 follows the same path. Alice applies a phase shift to encode a bit value on this pulse P1 only. Due to rotation by the Faraday mirror pulse P1 is now reflected at the PBS into the long arm in Bob where he applies a phase shift to make a basis set choice. The pulse P2 is transmitted at the PBS and both pulse P1 and P2 arrive at coupler C_1 at the same time to interfere. Single-photons detectors are used to determine which output the photon travelled through [31].

One of the disadvantages of this approach is that it is more susceptible to Trojan horse attacks. It is possible for Eve to send a probe beam and look at the reflections from the mirror at the end of Alice's system to gain information on the phase encoding. To counter such an attack Alice can add an attenuator to reduce the light in the system but this means such a system would not be compatible with single-photon sources. Due to the bidirectional nature of the system Rayleigh scattering is also a potential issue when the clock frequency is high which can cause an increase in the error rate in Bob [31].

2.5 Security discussion of quantum cryptography

2.5.1 Shannon information theory

One of the most important contributions of Claude Shannon to the area of information theory was contained in his paper "The Mathematical Theory of Communication" [3] where he introduced the concept of entropy into the field of information theory. From the second law of thermodynamics entropy is a measure of the randomness in a system and its value always increases. When applied to information theory this meant that many sentences can be dramatically shortened without losing their meaning. He proved that in a noisy communication, a signal could always be sent without distortion. If the message is encoded in such a way that it is self-checking, signals can always be received with the same accuracy as if there was no interference on the communication channel. Shannon showed that if the entropy rate, the amount of information you wish to transmit, exceeds the channel capacity then there were unavoidable and un-correctable errors in the transmission. If the entropy rate is below the channel capacity then there is a way to encode the information so that it can be received without errors. This is true even if the channel distorts the message during transmission. In Shannon's paper he introduced two important theorems, the noisy coding theorem and the noiseless coding theorem. As a simple example of the noiseless theorem can be understood by considering the following message:

TXT MSSGS SHRTN NGLSH SNTNCS

It is still possible to correctly read the above message even though there are 11 vowels missing. The noiseless coding theorem tries to quantify how much redundancy can be introduced and still the message can be decoded without errors. In communications redundancy is used to combat errors. The noisy coding theorem quantifies how much redundancy is needed in a message in order to correct errors introduced by noise present in a communication channel [32].

In the area of cryptography Shannon showed that the one-time pad achieves perfect secrecy if Alice and Bob share a secret key that is as long as the message to be encrypted.

2.5.2 Error correction, reconciliation and privacy amplification

The basic quantum key distribution protocol is inadequate in practice because realistic detectors have noise which results in Alice's and Bob's data differing even without the presence of an eavesdropper. When the quantum transmission is complete Alice and Bob must exchange a public message which enables them to reconcile the differences between their data. One of the most common methods of error correction is the Cascade error correction code [33]. Cascade is easily implemented and has the added benefit of information leakage which is close to the theoretical limit shown in Figure 2.16. Other methods include a low density parity check (LDPC) and Winnow. Although Cascade requires a lot more two-way communications than Winnow, Cascade is more efficient at error rates up to 10% and is therefore more commonly used in QKD systems [15]. The first step of the Cascade error correction protocol is that Alice and Bob publically agree on a permutation of their bits. The shuffled strings are then portioned into blocks of size k in such a way that it is believed that it contains no more than one error. Next Alice and Bob publically compute and compare the parity bits of each block. If the block contains an error, a difference in parity is detected. With this method an odd number of errors are detected but even numbers remain undetected. If a block has an unequal public parity the block is searched using a *bisective* search to locate the error and corrected. In order to locate and correct blocks with an even number of errors in them Alice and Bob then repeat the randomising and partitioning step for several passes with increasing block sizes for each pass. To correct further errors Alice and Bob continue to compare the parities of randomly chosen subsets of bits. If a parity mismatch is detected a similar procedure described above is performed to locate and

correct the error. The last bit of each random subset is deleted to avoid information leakage [34].

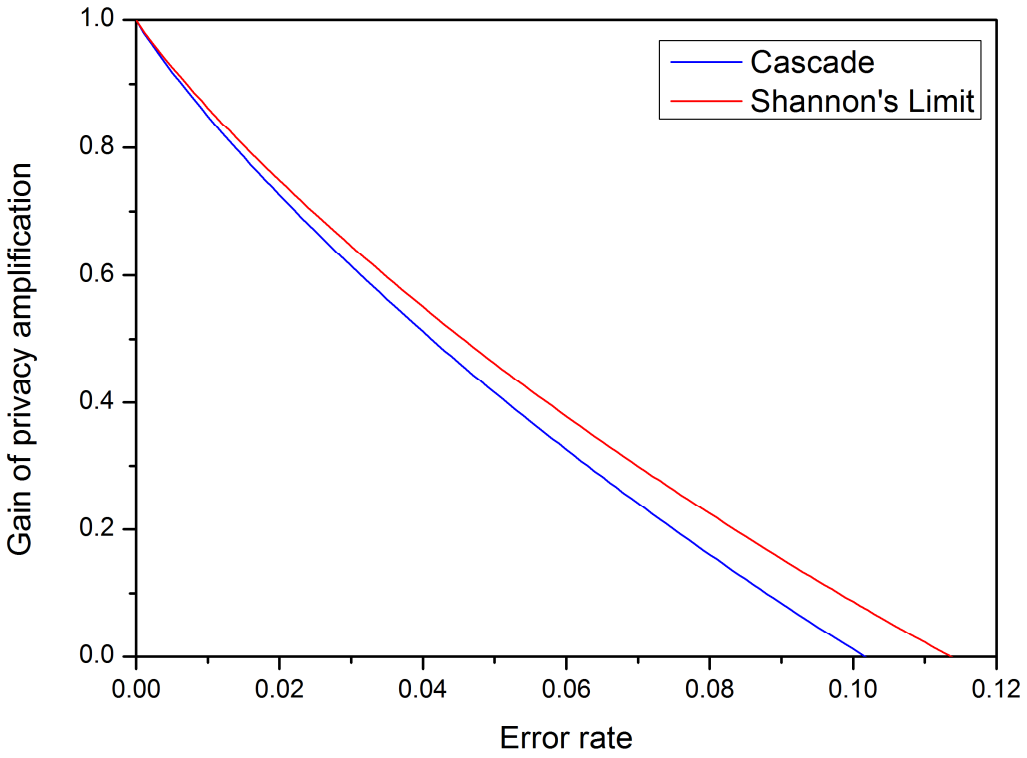

Figure 2.16. The gain for privacy amplification against increasing error rate is shown for the Cascade error correction protocol and for the theoretical Shannon's limit. The maximum error rate allowable for Cascade is about 10% while it is about 11% if the Shannon limit is obtained [34].

The efficiency of the error correction is given by the Shannon limit and it gives the minimum number of bits which must be revealed about the correct key to reconcile an error rate e [35]. The Shannon limit can be given in terms of the amount of Shannon information $I_s(e)$ contained in the final version of the key and is given by

$$I_s(e) = 1 + e\log_2(e) + (1-e)\log_2(1-e) \qquad \text{Equation (2.12)}$$

The minimum number of bits needed to correct a key whose length is n is given by

$$n_{\min} = n\left(1 - I_s(e)\right) \qquad \text{Equation (2.13)}$$

The last step in a quantum cryptography protocol is called privacy amplification which was first described by Bennett *et al.* in 1988 [36] and is an attempt to reduce Eve's information about the key. For this step Alice randomly selects pairs of bits and computes their parity. Unlike in error correction she does not publically announce the parity value but only the bits which were used. Alice and Bob then replace the two bits

by their value of the parity. The key length is shortened but if Eve has only partial information on the two bits, her information on the value of the parity is even less [17].

2.6 Eavesdropping in QKD

The BB84 protocol allows Alice and Bob to share a secret key. In the simplest case, if an eavesdropper attempts to measure an unknown quantum state sent from Alice and resends it to Bob she will introduce unavoidable errors in the system due to the Heisenberg uncertainty principle. Alice and Bob can look at their error rate for transmission (quantum bit error rate) and decided if it is safe to continue the key generation. It is generally assumed in eavesdropping attacks that Eve has perfect technology and is only limited by the laws of quantum mechanics. The eavesdropping strategies can be divided into three categories, individual attacks, collective attacks and joint attacks. The individual attack is a strategy in which Eve attaches independent probes to each quantum state and measures each probe independently. In collective attacks Eve probes each quantum state independently but she measures the whole set of probes jointly. In a joint attack Eve can probe all the quantum states jointly and is the most general attack on the quantum channel. It is generally assumed that for joint and collective attacks Eve measures her probe after Alice and Bob have completed all public discussion about basis reconciliation, error correction and privacy amplification [17].

2.6.1 Eavesdropping attacks

2.6.1.1 Photon number splitting (PNS) attacks

By using a strongly attenuated coherent source in a quantum cryptography system allows Eve to perform a type of attack called the beam splitting attack. This attack results from the multiphoton probability from a weak coherent pulse and the loss in the transmission line. In Quantum cryptography experiments the mean photon number per pulse is usually 0.1 which means that about 1 in 10 pulses contain only photon and 1 in about 200 pulses contain two or more photons. The eavesdropper can use this to tap off a fraction of the signal by means of a beamsplitter so that in some cases both Bob and Eve each receive a photon. If a polarisation encoding scheme is used both Bob and Eve can receive the photon such that the polarisation state remains undisturbed. If Eve can store the photon until Bob publicly announces the representation that he choose she can then use this information to perform a measurement in the same basis announced by Bob and she is able to obtain some of the key. The transmission of the key becomes

completely insecure with a high channel loss as Eve can replace it with a lower loss one [37]. For four state protocols like BB84, Eve can obtain full information from three-photon pulses using unambiguous discrimination techniques [38]. She can measure the total number of photons in each signal state by performing a *quantum non-demolition* measurement which does not introduce any error on the signal [39].

2.6.1.2 Intercept resend attack

The intercept-resend attack is an attack in which Eve measures the photons emitted from Alice and then retransmits the measured photons via a lossless quantum channel. Eve measures each qubit in one of the two basis sets for the BB84 protocol in the same manner as Bob would perform. She then sends another qubit in a state which corresponds to her measurement result. In 50% of the time she measures in the correct basis set and then transmits the qubit to Bob. In this occasion the eavesdropper in not detected by Alice or Bob. However 50% of the time she measures the qubit in the wrong basis set and transmits this to Bob. In this case after Alice and Bob eliminate the cases where they used incompatible basis sets they obtain a 25% error in their sifted key which alerts them to the presence of an eavesdropper [17].

2.6.1.3 QKD security attacks based on imperfect detectors

Very recently attacks on QKD systems have concentrated on using design imperfections in single-photon avalanche photodiodes (APD) [40]. The operation of these devices is discussed more thoroughly in section 2.11. These attacks are not based on any flaws in the cryptographic protocol but only on the engineering implementation as QKD has already been proved to have unconditional security. APDs are operated in Geiger mode, in the case of Si-APD (Perkin Elmer) they are biased by a high voltage source through a 360 kΩ bias resistor about 10 volts above the breakdown voltage (Figure 2.17). Two stray capacitances in the device help in the operation. When there is no current following in the APD the capacitors are biased at the bias voltage. During an avalanche process the capacitors quickly discharges through the APD which produces a short current pulse. When the voltage at the APD drops below the bias voltage the avalanched is quenched and the capacitors are slowly recharged through the bias resistor. While the capacitors are charging the detectors are insensitive to single-photons. A photon which arrives before the capacitors are fully charged can reset the voltage but without causing the detector to click. In this way the detector can be blinded indefinitely. In this attack scheme Eve makes use of the intercept resend attack which allows her full knowledge of Bob's systems. She intercepts the state which Alice

transmits but she has a 50% chance of measuring in the correct basis set. She sends the state not at the single-photon level but instead sends bright trigger pulses which enables her to force Bob's detector to click only when he measures in the same basis set as Eve and with the correct bit value. Lydersen's group demonstrated this attack on the comerically available id3110 Clavis2 and QPN 5505 QKD systems from IDQuantique [41]. Using bright light illumination they managed to successfully blind gated InGaAs/InP avalanche photodiodes (APD) which converts them to classical linear detectors. In this way the detector are fully controllable by classical laser pulses superimposed over the bright continuous-wave illumination. Subsequently work by Yuan *et al.* [42] sought to eliminate this security loophole in QKD. Their work focused on the bias resistor in the APD. A photon is detected if the voltage drop across the sensing resistor R_s exceeds the discriminator voltage level which ideally is set as low as possible. Yuan *et al.* showed that the range of continuous wave input powers over which the detector is blind to single-photons narrows as the bias resistor R_s is decreased. For most gated Geiger mode APDs this resistor is redundant and can be removed therefore eliminating the blinding attack.

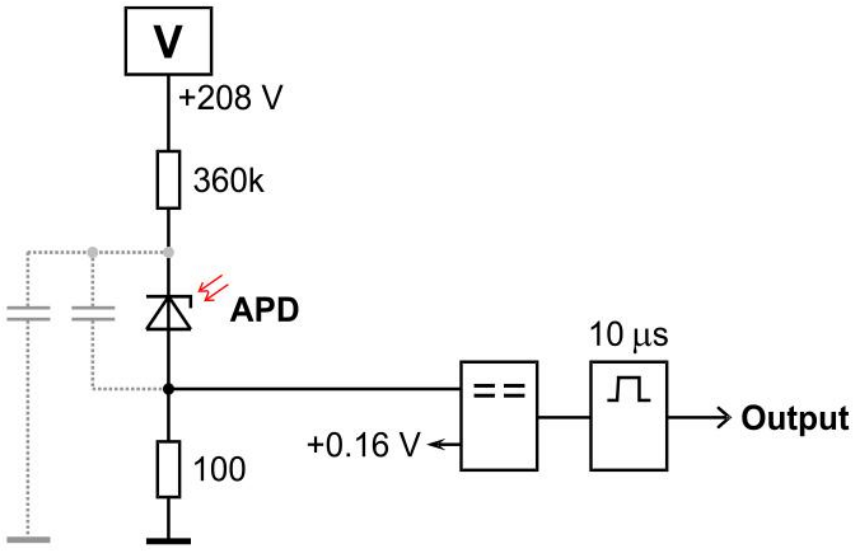

Figure 2.17. Equivalent circuit diagram for APD. The two stray capacitors are shown to the left [42].

2.6.1.4 Time shifted attacks

Another form of attack which can be used to gain an eavesdropper information on the shared key is via the time-shifted attack [43]. This has shown that there is a non-zero probability (4%) of breaking the security of the QKD system. This form of attack relies

on the fact that most if not all QKD systems will have at least two detectors and each will have a slight difference in the detection efficiency. This detection can vary as a function of time, frequency, polarization or spatial information. Eve has the ability to manipulation one of these variables to slightly change the detection efficiency at her choosing. In QKD it is assumed that Bob's detector will have an equal number of binary "1" and "0" values but this is not necessary the case under such an attack. Eve has the ability to time delay the signal so that in the case of a two detector system, detector 1 and detector 2, she can delay the signal so that the photons arrive at Bob when detector 1 has higher detector efficiency than detector 2 thereby manipulating the number of binary ones and zeros that Bob receives. The time-shift attack can also be more generalised to spatial, spectral, and polarisation-shift attacks which also make use of the detection efficiency mismatch.

2.6.1.5 Trojan horse attacks

Instead of Alice attempting to gain information about the quantum states sent between Alice and Bob it is also possible for her to send signals into Alice's and Bob's systems through the quantum channel. Eve can send bright pulses of light into their systems and analyse the back-reflected light in an attempt to gain information about which detectors fired or the settings of phase and polarisation modulators. The "*plug-and play*" system is particular susceptible to this attack as light is reflected off Faraday mirrors in Alice's system back to Bob [17].

2.6.2 GLLP security analysis

The work of Gottesman, Lo, Lütkenhaus and Preskill (GLLP) produced a security analysis which deals with imperfective devices and sources for QKD systems. In their paper they introduce the concept of tagged and untagged qubits. Fred, an adversary working with Eve can attached to each qubit from Alice a tag which allows Eve to know which basis set the qubits were prepared in. Tagged qubits are unsecure for QKD because their basis choice encoding is revealed to Eve. These bits have been attacked without any visible errors. Δ is the fraction of qubits that have been tagged. Of the remaining $1-\Delta$ pulses (untagged) these can suffer phase errors due to Eve's interaction. In the BB84 protocol untagged qubits are those which are generated by single-photons and tagged qubits are generated from multi-photon pulses [44]. In GLLP post processing error correction is applied by Alice and Bob to all the qubits. A fraction of the bits given by $H_2(\delta)$ are sacrificed during error correction, where δ is the bit error.

Of the remaining $1-\Delta$ key elements $(1-\Delta)h\left(e_{untagged}^{ph}\right)$ have to be removed for privacy amplification where $e_{untagged}^{ph}$ is the phase error rate. In the worst case scenario all the errors are on the untagged key elements therefore $e_{untagged}^{ph} \to \delta/1-\Delta$ [15]. The final secure key generation rate is given by Equation (2.14).

$$R = \max\left((1-\Delta) - H_2(\delta) - (1-\Delta) H_2\left(\frac{\delta}{1-\Delta}\right), 0 \right) \qquad \text{Equation (2.14)}$$

In GLLP analysis the net key generation rate is $O(\eta^2)$, where η is the overall transmission probability of the channel. For many QKD experiments the choice of μ of 0.1 photons per pulse is chosen. In most cases this value is arrived at arbitrarily. Lütkenhaus looked at this problem and found that for weak coherent pulses the optimum μ value depended on the both the detector efficiency and the loss of the quantum channel. The optimum value is given by

$$\mu_{opt} \approx \eta_B \eta_T \qquad \text{Equation (2.15)}$$

where η_B is Bob's detector efficiency and η_T is the transmission efficiency of the quantum channel. This means that as the transmission distance is increased between Alice and Bob μ must be decreased accordingly for security against the photon number splitting attack [45].

2.6.3 Decoy states

The security of quantum key distribution is guaranteed by fundamental laws of quantum physics. However in real world applications this security is compromised by imperfect instruments. Qubits are often encoded using highly attenuated lasers but the finite probability of the signal containing multiphoton pulses leaves the system vulnerable to possible eavesdropping attacks. When preforming a full security analysis the secure key generation rate can be dramatically reduced by the presence of multi-photons as only qubits encoded on signal photons are guaranteed to be secure. The use of decoy states offers the opportunity to increase the secure key generation rate without much additional complexity in the experimental apparatus. In this method Alice has the ability to prepare her qubits and then turn her power up or down for each signal that she transmits by the use of a variable optical attenuator. The basic principle involves Alice randomly replacing pulses from the signal source by multiphoton pulses (decoy pulses). Eve does not have the ability to distinguish multi-photon pulses of the signal from those

of the decoy which means that the yields from these must be similar. Alice and Bob can detect the photon number splitting (PNS) attack by monitoring the yield of the decoy pulse. The number of photons that Alice prepares for the signal state follows a Poissonian distribution. The secure key generation rate for decoy states is given by

$$S = q\left\{-Q_\mu f\left(E_\mu\right)H_2\left(E_\mu\right)+Q_1\left[1-H_2\left(e_1\right)\right]\right\} \qquad \text{Equation (2.16)}$$

where q depends on the QKD implementation, Q_μ and E_μ is the gain and QBER of the signal state, e_1 is the QBER of detection events by Bob from single–photon signals from Alice, $f\left(E_\mu\right)$ is the efficiency of the error correction, H_2 represents the Shannon entropy function and Q_1 is the gain for the single-photon state [46]. Alice and Bob can experimentally measure Q_μ and E_μ and if they know certain properties of the channel loss any eavesdropper will with a high probability change these values. Shown in Figure 2.18 is the comparison of the secure key generation rate with and without decoy states using experimental values used by Gobby *et al.* [47]. In decoy states the key generation rate scales as $O(\eta)$ which leads to a dramatic increase in the key generation rate compared to the case with decoy states.

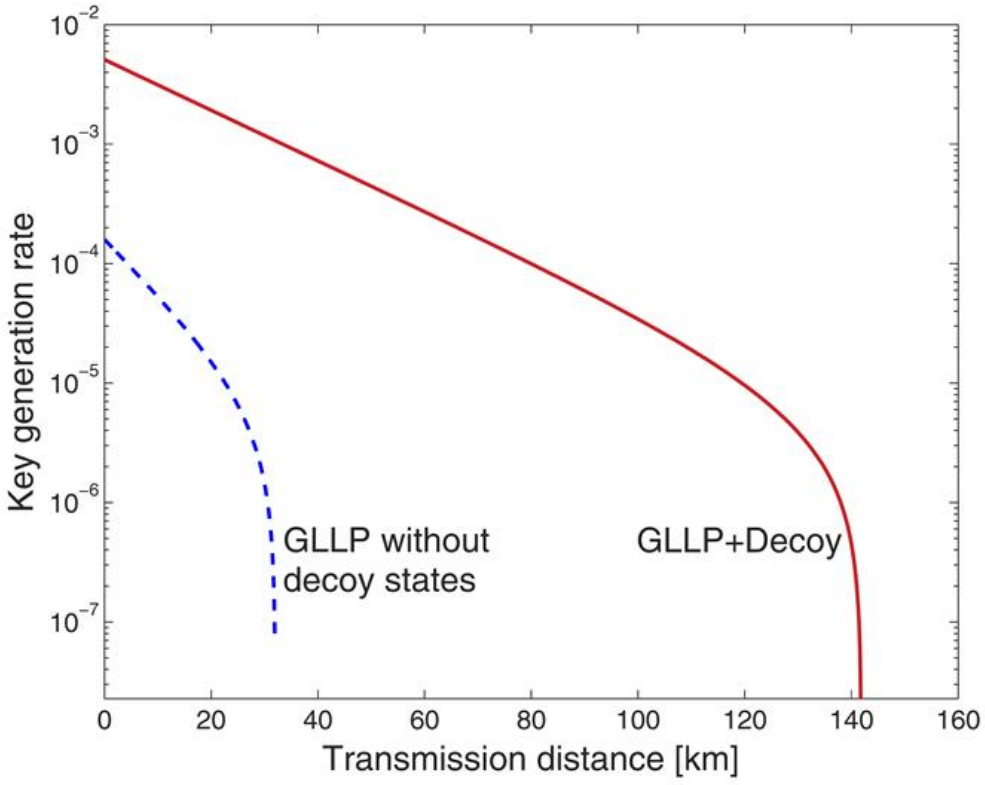

Figure 2.18: Effect of secure key generation rate with and without decoy states [48].

2.7 Important experimental QKD systems to date

There has been rapid progress in the field of quantum key distribution ever since the first practical demonstration was made back in 1992 [49]. Although the free space quantum channel was only 32 cm in length it never the less opened the field for further experiments. In 1994 work published by Gisin's group from the University of Geneva described an all-fibre quantum cryptography QKD system based on polarisation encoding [50]. However, such a system was limited due to the intrinsic birefringence of an optical fibre, polarisation mode dispersion and polarisation dependent loss. In the same year Paul Townsend demonstrated a QKD system operating at a wavelength of 1.3 μm using phase encoding of the photons [51]. Such a system used a cascaded Mach-Zehnder interferometer arrangement which required polarisation monitoring at the receiver to ensure that birefringence effects in the fibre did not degrade the visibility. In 1996 Jacobs and Franson demonstrated [52] a free space QKD system under daylight operation. The technique adopted was similar to the approach already used for fibre systems with the addition of collimating optics for the free space transmission and optical filtering techniques to remove background light. In 1996 Gisin's group in Geneva introduced the concept of "*plug- and-play*" system for QKD which also employed fibre interferometry but without the need for active polarisation control [31]. Such as system was susceptible to a Trojan horse attack in which an Eavesdropper could gain information on the state of Alice' modulator by shining light into the quantum channel and looking at the reflected light from Alice [53].

The first demonstration of a single-photon source for use in QKD was performed by Philippe Grangier's group in France in 2002 [54]. This experiment operated in free space and used nitrogen vacancies in diamond as the source of single-photons, which operated at room temperature. This system achieved bit rates of 7700 bits/sec and a quantum bit error rate less than 4.6% over a distance of 50 m. Later that same year researchers at Stanford University demonstrated QKD using a single quantum dot located in a microcavity. The sample was held between 5-10 K and was optically excited with a repetition rate of 76 MHz. They reported a $g^2(0)$ of 0.14. A final key generation rate of 25 $kbits^{-1}$ was obtained over a free space link of 1 metre [55].

In 2005 Lo, Ma, and Chen working in the University of Toronto introduced the idea of decoy state QKD which could be used to extend the distance at which keys could be securely distributed [46]. The first experimental demonstration using decoy states was

performed the following year by the same group [56]. The experiment employed an acousto-optic modulator to vary the intensity of the pulses sent by Alice. To date the method of decoy states have enabled quantum keys to be transmitted with the highest bit rates, with 1 Mbit/sec over 20 km of fibre and 10 kbits/sec over 100 km [57].

In 1991 Ekert proposed a QKD scheme based on entangled pairs of photons [28]. The security of the system could be tested using the Bell inequality. The first demonstration of two photon entanglement over a large distance was performed by Tittel *et al.* in 1998 [58]. Violation of Bells inequality was observed by 10 standard deviations over a distance of 10.9 km. In 2000 Jennewein reported the first entangled based QKD system operating over 360 m of optical fibres producing raw rates of between 400-800 bits/sec [59]. In 2007 Ursin *et al.* demonstrated a free space entanglement based QKD system in the Canary Islands over 144 km [60]. Operating over this distance acted as a test for future possibilities communicating from a low-Earth-orbit satellite to two different ground stations.

The first gigahertz QKD system operating in fibre was performed by Gordon *et al.* in 2004 [61]. The system used polarisation encoding to implement the B92 protocol. The system operated at a wavelength of 850 nm employing commercially available Si single-photon detectors which ensured a detection efficiency of ~40% at this wavelength. A net bit rate of 7 kbit/sec was achieved over a 10 km fibre.

QKD at telecom wavelengths have been demonstrated recently using semiconductor APDs and superconducting detectors. In 2007 a differential phase shift QKD (DPS QKD) system using superconducting single-photon detectors was demonstrated. The system generated keys at a rate of 12.1 bits s^{-1} over a 200 km reel of fibre with a clock frequency of 10 GHz. The system operated at 1550 nm where the detection efficiency was 0.7% [62]. In 2008 Shields *et al.* demonstrated a 1 GHz system using InGaAs APDs operating in self-differencing mode using phase encoding with asymmetric Mach-Zehnder interferometers. They obtained a secure bit rate of 2.37 Mbit s^{-1} at 5.6 km and 27.9 kbits s^{-1} at 65.5 km [63].

QKD has now advanced to such a stage now where there are many commercial systems available. ID Quantique, a commercial spin off from the Group of Applied Physics in the University of Geneva, using their Cerberis QKD system was used to secure a point-to point Ethernet link to send ballot information from the central ballot counting station

to the Geneva government data centre [15]. Other commercial companies include MagiQ based in New York and Quintessence in Australia.

In June 2004 the DARPA Quantum Network became the world's first quantum cryptography network linking BBN Technologies to Harvard and Boston Universities. The network uses a variety of QKD technologies including weak coherent pulses for phase encoding, polarisation entangled photons and a free space QKD system [64]. Another notable QKD network was the European funded Secure Communication based on Quantum Cryptography (SECOQC). It was built to overcome the issue of QKD links only being able to operate over point-to-point connections between two users. The SECOQC network was designed to use a variety of QKD implementations including coherent one-way, entanglement based and free space systems. The SECOQC prototype in Vienna consisted of six nodes connected by 8 QKD links at distances greater than 25 km in standard telecoms fibre obtaining a key generation rate of 1 $kbits^{-1}$ [65].

2.8 Photon sources for QKD

2.8.1 Weak coherent pulses

Quantum cryptography, when implemented correctly makes use of single-photon Fock states. In quantum mechanics a Fock state is any state with a well-defined number of particles [66]. In real life these are difficult to implement. Practical implementations involve using faint laser pulses in which the photon and the photon number distribution obey Poissonian Statistics due to its discrete nature. Coherent states which use low photon numbers can be implemented using semiconductors and calibrated attenuators. The probability of finding n photons in a weak coherent state is given by

$$P(n,\mu) = \frac{\mu^n}{n!} e^{-\mu} \qquad \text{Equation (2.17)}$$

Poisson distributions are characterised by their mean value μ. Figure 2.19 shows the Poisson distribution for $\mu = 0.1$, 1, 5 and 10. As the value of μ decreases the width of the distribution decreases and its peak increases. The standard deviation for a Poisson distribution is given by

$$\Delta n = \sqrt{\mu} \qquad \text{Equation (2.18)}$$

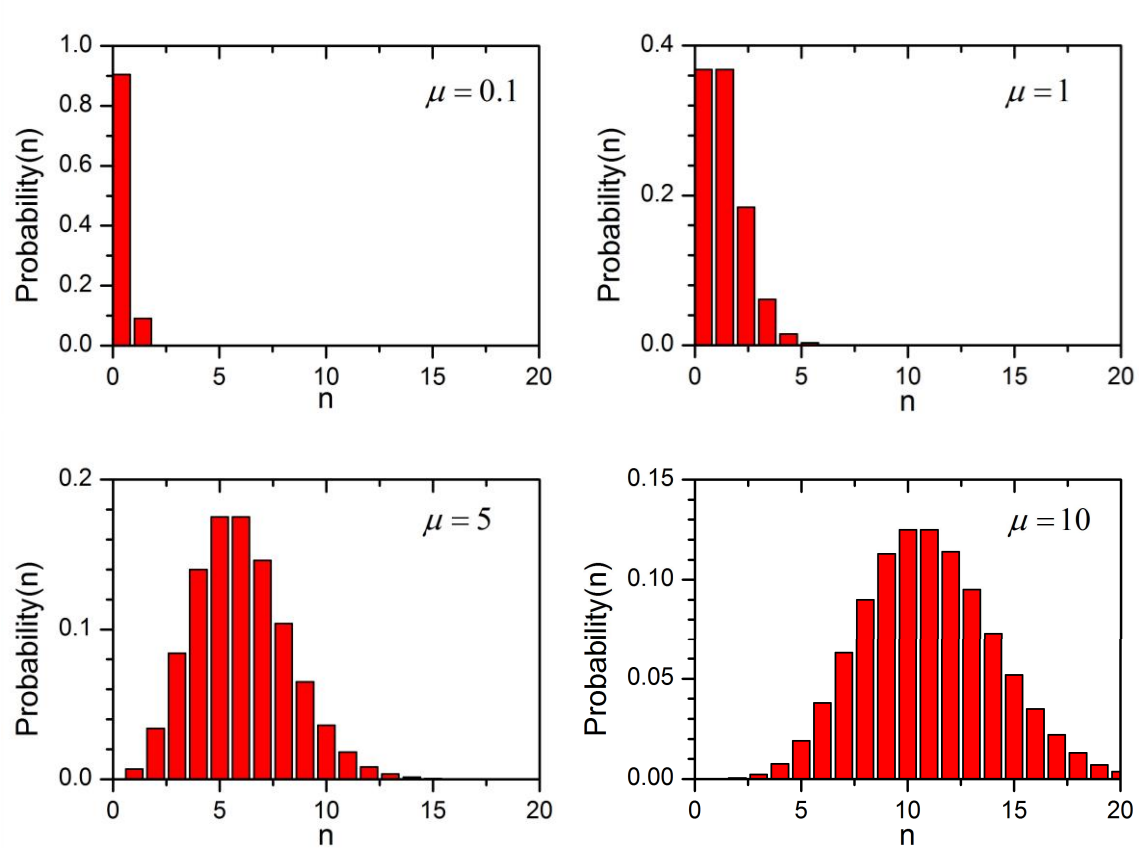

Figure 2.19. Poisson distributions for mean values of 0.1, 1, 5 and 10. Distributions obtained using Mathcad.

Many quantum key distribution systems use a mean photon number per pulse of 0.1. However using Equation (2.18) we can see that there is non-zero probability that a given pulse may contain more than one photon.

$$P(n>1 \mid n>0,\mu)=\frac{1-P(0,\mu)-P(1,\mu)}{1-P(0,\mu)}=\frac{1-e^{-\mu}(1+\mu)}{1-e^{-\mu}} \qquad \text{Equation (2.19)}$$

In fact 5% of the nonempty pulses contain more than one photon, as shown in Figure 2.20, and the choice of μ depends on the transmission loss of the system [45]. One of the drawbacks of weak coherent sources is that when μ is small most of the pulses are empty. This leads to a decrease in the bit rate for communication purposes. This decrease can be overcome nowadays thanks to the gigahertz modulation rate of telecommunication lasers. This problem becomes more of an issue operating at longer wavelengths. Detectors which operate in this wavelength suffer from a huge increase in the noise when operated at high frequencies. This effect limits the use of low photon numbers smaller than 1% [67], [68], [69].

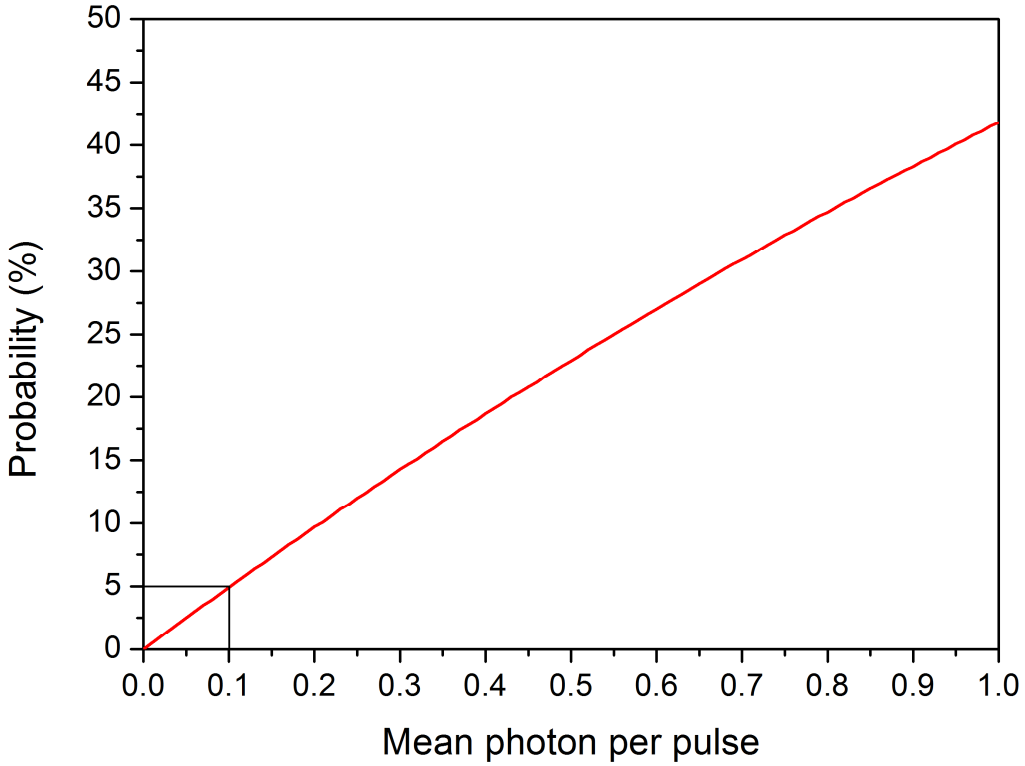

Figure 2.20. The probability that a pulse contains n>1 photons using Poissonian photon statistics. Using μ =0.1 there is a 5% probability that the pulse contains n>1 photons.

2.8.2 Quantum dots

A quantum dot is an engineered structure which is used to confine the movement of carriers in all 3 dimensions which leads to quantisation of the available energy levels. It is possible to obtain single-photon emission from a quantum dot if one of the available energy transitions is selected. The density of states of a semiconductor is given by

$$g(E)dE = N(E)dE \qquad \text{Equation (2.20)}$$

where $N(E)$ is the probability of occupancy of a state with energy from E to $E+dE$. The equation for the energy of the electron in terms of its k vector is given by the following expression

$$E = \frac{\hbar^2}{2m}\left(k_x^{\,2} + k_y^{\,2} + k_z^{\,2}\right) \qquad \text{Equation (2.21)}$$

In classical physics all values of energy would be allowed since there are no restrictions on the number of electrons with the same k value. On the atomic scale quantum mechanics comes into effect. The wave function of the electron has to satisfy the

Schrödinger wave equation and as a consequence for a quantum dot the values of k take the form of

$$k_x = \frac{2\pi n_x}{L},\ k_y = \frac{2\pi n_y}{L}, k_z = \frac{2\pi n_z}{L}$$

where n_x, n_y and n_z are integer values. Therefore in a 0-dimensional structure the values of k are quantised in all three directions. The available states exist at discreet energies and can be represented by a delta function. In real quantum dots the size distribution leads to a broadening of the line function [70]. Figure 2.21 shows the density of states for various dimensional structures.

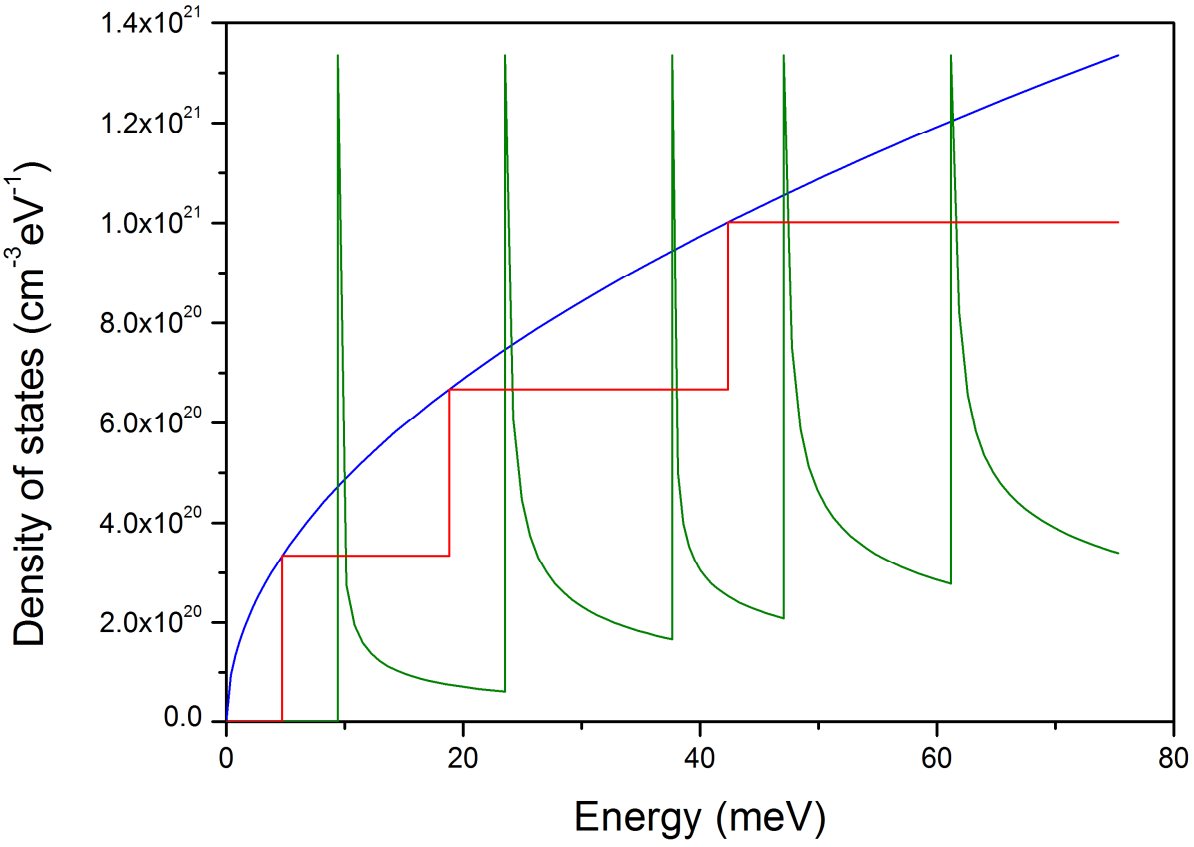

Figure 2.21 Density of states per unit volume verses energy for a 3-D semiconductor (blue curve), a 10 nm quantum well with infinite barriers (red curve) and a 10 nm by 10 nm quantum wire with infinite barriers (green curve). $m^*/m_0 = 0.8$

Semiconductor quantum dots can be used as a source of single-photons. They have the advantage of narrow spectral line width and can be integrated into devices structures such as p-n junction and resonator configurations [71]. Due to the high refractive index contrast ratio between the semiconductors and the air few photons can escape the structure. The extraction efficiency can be increased by embedding the quantum dot in

a microcavity. A quantum dot can be placed into a Fabry-Perot cavity which has the effect of changing the energy available to the emitted photon [72]. This is because the cavity only supports certain standing waves depending on the dimensions of the cavity. At resonance when the dot emits at the same wavelength as the cavity mode the photon emission rate increases accompanied by a decrease in the decay time. This is called the Purcell effect. The Purcell enhancement is a low temperature effect as at higher temperatures the enhancement factor is diminished when the spectral linewidth of the emitter becomes much larger than the linewidth of the cavity [73].

The standard technique of growth of quantum dots is by the Stranski-Krastanow method, also known as the process of self-assembly [72], [74], [75]. Quantum dots are grown this way when heterostructures are grown with slight lattice mismatch. The lattice mismatch creates strain in the structure which is relieved by the formation of small islands. It is the formation of these islands that form the quantum dots [76], [77]. The layer containing quantum dots can be fabricated using molecular beam epitaxy (MBE) or metal oxide chemical vapour deposition techniques (MOCVD). When quantum dots are fabricated they are arrange randomly on the substrate surface which represents a problem when the application requires the addressing of an individual dot. Nanometre scale site control has been demonstrated using scanning tunnelling microscope assisted nanolithography together with self-organising molecular beam epitaxy [78]. A further discussion of quantum dots is contained in Chapter 3.

2.8.3 Vertical cavity surface emitting laser (VCSEL)

A vertical cavity surface emitting laser (VCSEL) is a type of semiconductor laser whose emission is perpendicular to the surface, contrary to traditional edge emitting lasers where the resonant cavity is in the plane of the active layer. The first operation of a VCSEL was first demonstrated by Soda *et al.* in 1979 [79]. The light resonates between mirrors on the top and bottom of the laser wafer (see Figure 2.22) so that photons pass through only a very short length typically <1 μm of active medium. VCSELs have much lower round trip gain than horizontal edge emitting lasers and as a result they require high reflectivity mirrors. The laser resonator consists of two distributed Bragg reflector mirrors consisting of several alternating $\lambda/4$ layers of AlAs and AlGaAs. VSCELs have a rotationally symmetric beam profile and low threshold currents. They are available in the wavelength 650-690 nm using GaAs/GaAlAs and from 850-980 nm using InGaAs/GaAs [80], [79], [81], [82]. VCSELs operating at speeds of up to 40

Gbits/second have now been reported making them very useful in modern optical communication systems [83]. Highly attenuated VCSELs have been used in many quantum key distribution systems [84], [85], [86].

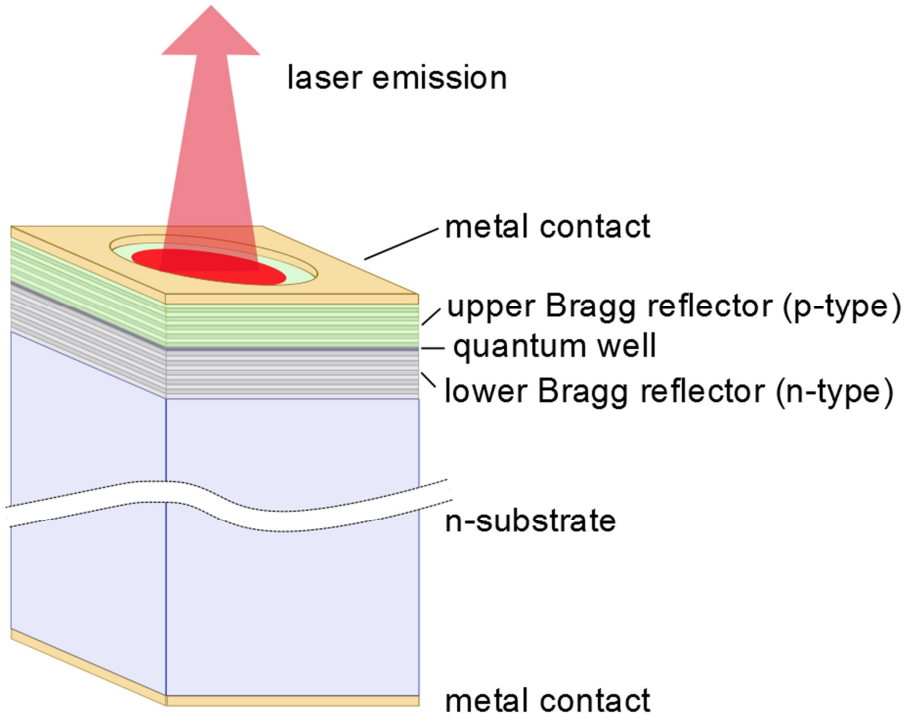

Figure 2.22. Structure of VCSEL laser. Quantum well layer is contained between two Bragg reflectors with light emission perpendicular to the surface.

2.8.4 Heralded single-photon source

Single photons which are produced in pairs without any intra-pair correlation are useful in quantum information. This technique is based on the probabilistic emission of correlated photon pairs, and heralds the presence of one photon by the detection of the second photon of the pair. These heralded single photon sources are produced by either spontaneous parametric down-conversion (SPDC) [87], [88] or by four wave mixing [89], [90]. In spontaneous parametric down conversion a pump photon is split in a nonlinear crystal into two photons, an idler and a signal photon. Energy $1/\lambda_{pump} = 1/\lambda_{signal} + 1/\lambda_{idler}$ and momentum $k_{pump} = k_{signal} + k_{idler}$ conservation laws are obeyed. If the two photons produced have the same polarisation the process is called Type I SPDC or if they have perpendicular polarisation it is referred to as Type II SPDC. Heralded single photons at a wavelength of 1550 nm using SPDC was demonstrated by Soujaeff *et al.* producing photons at a rate of 2.16×10^5 photons per second [91]. Recently in 2008, Hayat *et al.* observed the first two-photon emission

from optically pumped bulk GaAs and in electrically driven GaInP/AlGaInP quantum wells [92]. Two-photon emission is a process in which an electron transitions between quantum levels via the simultaneous emission of two photons. This process was reported to be three orders of magnitude more efficient the existing down-conversion schemes which would have many interesting quantum applications such as photon entanglement. Four wave mixing is a nonlinear effect that results from the third order nonlinearity coefficient $\chi^{(3)}$ and results when two frequencies propagating through a nonlinear medium to produce two additional frequency components.

2.8.5 Nitrogen-vacancy single-photon source

Single nitrogen vacancies (N-V) in diamond are a promising option for producing non–classical light in the 600-800 nm wavelength region. The N-V centres in diamond are formed by a substitutional nitrogen atom with a vacancy trapped at an adjacent lattice position [93]. An advantage of this approach is that the device can work at room temperature and the short decay time of the excited state [94]. However a potential disadvantage for some applications is that the emission from the N-V centre is broadband, often several hundred nanometres [95] and quite often the emission efficiency can be low, typically a few per cent [96].

2.9 Proving the existence of the quantum nature of light

In the 1950s, when Hanbury Brown and Twiss were working on a technique to increase the resolution of stellar interferometry they discovered that the intensity fluctuations from a light source falling on two photodetectors were correlated [97]. They found that the joint probability of photodetection $P_2(t,t+\tau)$ at time t and $t+\tau$ is greatest at $\tau = 0$ and falls to a lower constant value at times $\tau > \tau_c$ when dealing with a thermal source with a coherence time of τ_c. This was the first demonstration of bunching where photons from a classical light source arrive in bunches rather than at random times like a Poissonian source. Their experiment, shown in Figure 2.23, used the 835.8 nm emission line from a mercury lamp and split the light equally on a 50:50 half silvered mirror to be detected by two photomultiplier tubes whose output currents i_1 and i_2 were multiplied and integrated together electronically. The variations in the current, Δi_1 and Δi_2, were related to the fluctuations in the intensity $\Delta I_1(t)$ and $\Delta I_2(t)$. The output given by $\langle \Delta I_1(t) \Delta I_2(t) \rangle$ was monitored as a function of the distance d between the photodetectors. The split light had intensities given by

$$I_1(t) = I_2(t) = \langle I(t) \rangle + \Delta I(t) \qquad \text{Equation (2.22)}$$

where $\langle I \rangle$ is the average intensity and $\Delta I(t)$ is the intensity fluctuation. For time $\tau = 0$ the output was given by

$$\Delta \langle I(t) I(t+\tau) \rangle_{\tau=0} = \langle \Delta I(t)^2 \rangle \qquad \text{Equation (2.23)}$$

The quantity $\langle \Delta I(t)^2 \rangle$ will be non-zero and strong correlations are observed in the intensity fluctuations. For times $\tau > \tau_c$ the output is given by

$$\langle \Delta I(t) \Delta I(t+\tau) \rangle_{\tau > \tau_c} = 0 \qquad \text{Equation (2.24)}$$

which means that the intensity fluctuations are completely uncorrelated. The second order cross correlation function can be related to the intensities by the following expression

$$g^{(2)}(0) = \frac{\langle I(t) I(t+\tau) \rangle}{\langle I(t) \rangle \langle I(t+\tau) \rangle} \qquad \text{Equation (2.25)}$$

The value of $g^{(2)}(0) \geq 1$ for all values of τ. The preceding takes a semi-classical approach in which the light is treated as a classical wave where the detection process is governed by quantum mechanics. In quantum theory, electromagnetic fields associated with a beam of light are given by operators. The second order autocorrelation function in quantum theory is given by

$$g^{(2)}(0) = \frac{\langle \hat{a}_1^\dagger(t) \hat{a}_1^\dagger(t+\tau) \hat{a}_1(t+\tau) \hat{a}_1(t) \rangle}{\langle \hat{a}_1^\dagger(t) \hat{a}_1(t) \rangle^2} = \frac{\langle n_1(n-1) \rangle}{\langle \bar{n}_1 \rangle^2} \qquad \text{Equation (2.26)}$$

where $\hat{a}_1^\dagger$ and $\hat{a}_1$ are the annihilation and creation operators and n_1 is the number of photons in a mode with average number $\bar{n}$. For non-classical light with $\bar{n} = 1$, $g^{(2)}(0)$ is less than 1 [98].

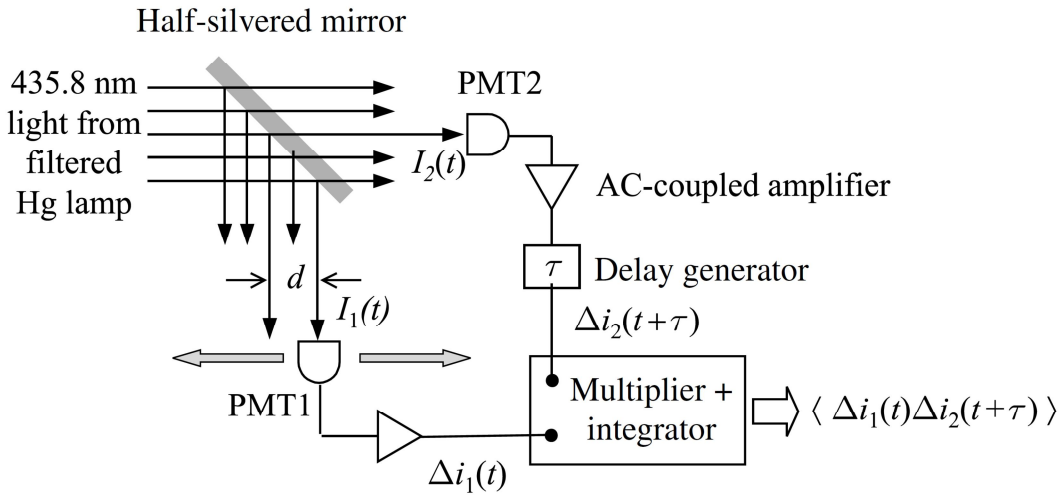

Figure 2.23. Hanbury Brown's and Twiss's 1957 experimental arrangement for the observation of bunching from a chaotic light source [66]. The detector PMT1 can be moved which is indicated by the horizontal grey arrows.

2.9.1 Hanbury Brown and Twiss experiment with single-photons

The Hanbury Brown and Twiss (HBT) experiment with single-photons is shown schematically in Figure 2.24. A stream of photons is incident on a 50:50 mirror and are divided equally to the two outputs. The photons are then collected onto detectors D1 and D2 are then recorded by an electronic counter/timer which simultaneously records the time between electrical pulses from D1 and D2 and the number of counts on each detector. The number of photons recorded on each detector is proportional to the intensity which allows the second order autocorrelation function to be written as

$$g^{(2)}(0)=\frac{\langle n_1(t)\,n_2(t+\tau)\rangle}{\langle n_1(t)\rangle\langle n_2(t+\tau)\rangle} \qquad \text{Equation (2.27)}$$

where $n_1(t)$ and $n_2(t)$ are the counts recorded on detector D1 and D2. $g^{(2)}(0)$ can be thought of as the conditional probability of detecting a second photon at a time $t=\tau$ given that we have already detected a photon at $t=0$. In the HBT experiment, when a stream of photons are incident on the beamsplitter they are randomly directed to D1 or D2. There is a 50% chance that a photon event will be recorded in D1 which starts the electronic timer. There is therefore zero probability of this same photon being recorded by D2 and stopping the timer and there will be no events at $\tau=0$. The next photon in the stream has a 50% chance of being recorded by D2 and stopping the timing electronics. If the pulse was recorded by D1 nothing happens as no stop signal was received. This process is repeated until a stop signal is recorded. No photon events are

expected at $\tau = 0$ while some events are recorded at for larger values of τ. A typical autocorrelation measurement on a pulsed single-photon emitter is shown in Figure 2.25(c).

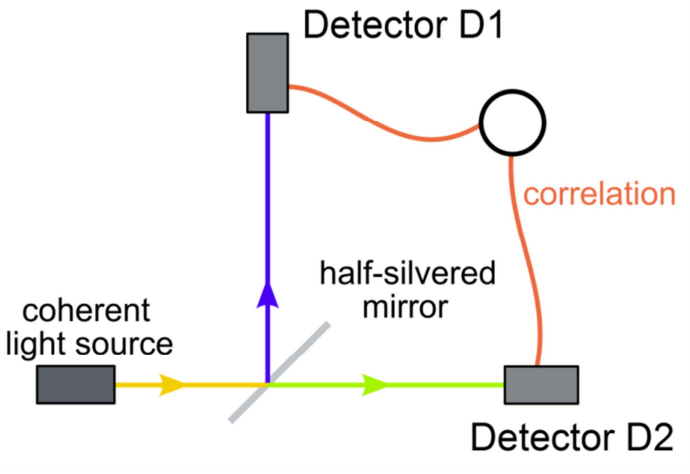

Figure 2.24. The experimental arrangement for the Hanbury Brown Twiss experiment.

2.9.2 Non-classical characteristics of a single-photon source

Figure 2.25 shows the second order autocorrelation functions for light sources with different photon statistics. For a coherent light source $g^{(2)}(0) = 1$ and for a bunched light source, such as the light from a discharge lamp, $g^{(2)}(0) > 1$.

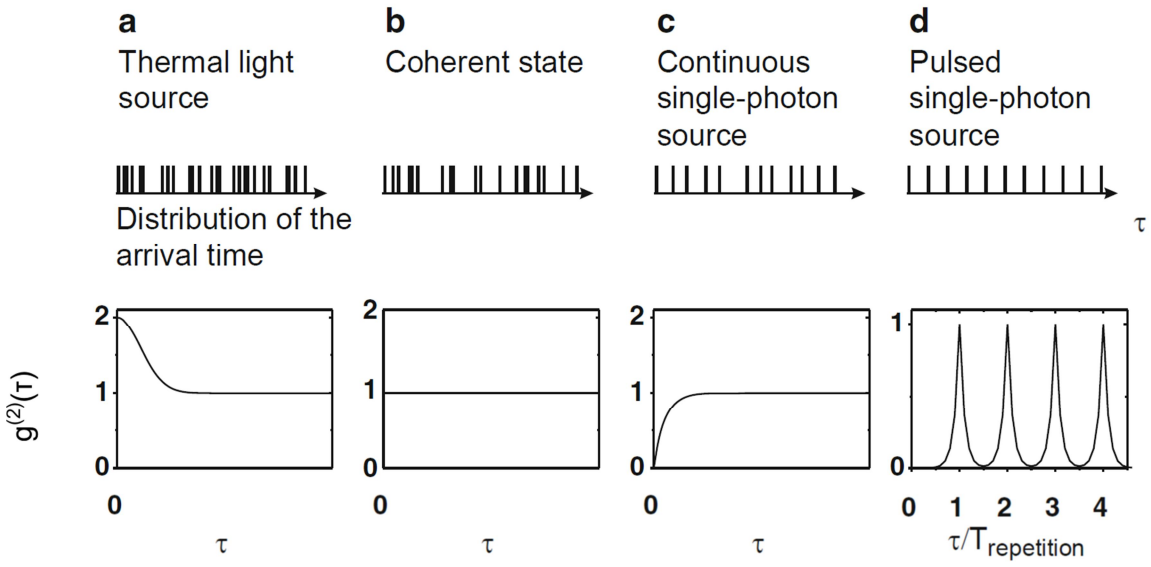

Figure 2.25. $g^{(2)}(0)$ function for a thermal light source (a), coherent light (b), continuous (CW) single-photon source (c) and a pulsed single-photon source (d). For a thermal and coherent state the photons are emitted with a random interval spacing while a single-photon source has a regular interval [99].

A light source with a $g^{(2)}(0) < 1$ is regarded as antibunched light in which the stream of photons are emitted with regular intervals between them as opposed to a random spacing. To obtain a light source with such properties we must look at the emission from a *single atom*. Antibunching is not observed with a large ensemble of atoms because the emission and excitation process are different for each atom and are independent from each other. The antibunching characteristic curve in Figure 2.25(c) can be given by

$$g^{(2)}(\tau) = 1 - c\exp\left\{-\left[r + \left(\tau_{lifetime}\right)^{-1}\right]|\tau|\right\} \qquad \text{Equation (2.28)}$$

where c is a constant and r and $\tau_{lifetime}$ are the pump rate and lifetime of the excited state respectively [100]. For large pump rates the temporal width of the antibunching peak is reducing according to Equation (2.28). When this temporal width becomes comparable to the timing resolution of the detector the ability to resolve the peak is reduced which can lead to an artificial increase in the $g^{(2)}(0)$ value.

2.10 Quantum transmission medium

In a quantum key distribution system Alice needs to be able to send her qubits to Bob over a quantum communication channel. Optical fibres have been extensively used to date as this medium since first demonstrated by Townsend in 1994 [51]. Free space quantum key distribution has also been demonstrated by many groups [52], [101] which opens up the possible of line of sight QKD and also between ground stations and satellites.

2.10.1 Optical fibres

Light is guided in optical fibres due to the refractive index profile across the section of the fibre leading to total internal reflection. During the last 25 years significant research and development has been carried out to increase the distance over which light can propagate in fibres before it is attenuated to noise (Figure 2.26). In the early days impurity ions in the fibre was the major source of attenuation but using better manufacturing techniques, these impurities were removed. Nowadays the attenuation (Figure 2.26) is 0.35 dB km^{-1} at a wavelength of 1310 nm and 0.19 dB km^{-1} at a wavelength of 1550 nm [102], [103]. Losses in optical fibres are mainly due to Rayleigh scattering which has a λ^{-4} dependence and absorption losses mainly from impurities like OH^- and transition metals. At wavelengths greater than 1.6 μm the main absorption process is due to transition between the vibrational states of the lattice [104].

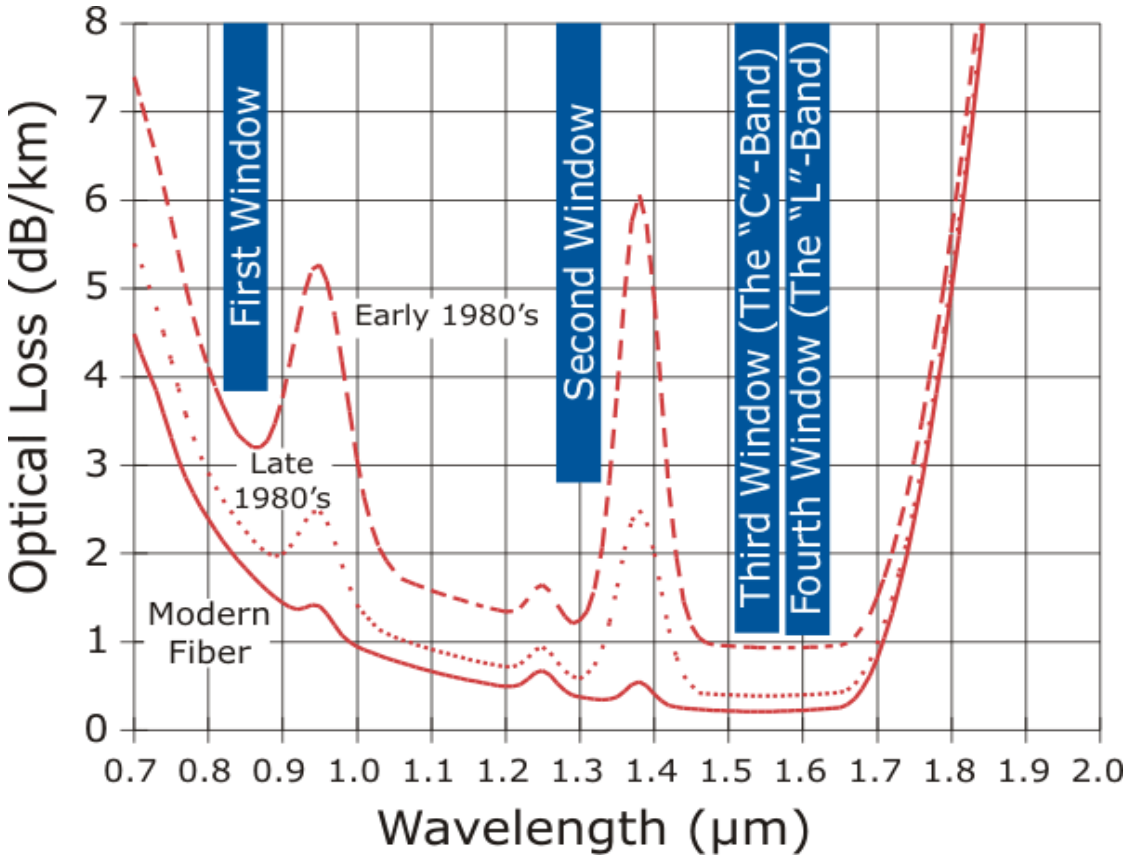

Figure 2.26. Attenuation of optical fibre throughout the last 30 years [105].

If the core of an optical fibre is large then many guided modes can propagate in the fibre. Such a fibre is called a multimode fibre. The cores of these fibres are typically 50 μm in diameter. Mode coupling is an issue in these fibres making them unsuitable as the quantum channel in quantum cryptography. When the core of the fibre is small enough that only one longitudinal mode can propagate this type of fibre is called a single mode fibre. At a wavelength of 1550 nm a fibre is single mode if the diameter is 8 μm. These fibres are suitable as the quantum channel in quantum cryptography. Whether or not a fibre can be classified as a single or multimode fibre can be determined by the following equation

$$V = \frac{\pi d}{\lambda_0}\left(n_1^2 - n_2^2\right)^{1/2} \qquad \text{Equation (2.29)}$$

where V is called the normalised frequency, d is the diameter of the fibre, λ_0 is the wavelength in the fibre and n_1 and n_2 are the refractive indices of the core and cladding. For a fibre to be classified as single mode $V < \pi/2$ [104], [106].

2.10.1.1 Fibre birefringence

Although many fibres are said to be single mode it is still possible for two orthogonally polarised modes to propagate in the fibre. In an ideal case the core of the optical fibre is

isotropic and both modes experience the same refractive index. However in real fibre due to birefringence affects, each mode experiences a slightly different refractive index. Birefringence is the presence of two different phase velocities for two orthogonal polarisation states. The effect is caused by asymmetries in the fibre geometry and stress around the core from manufacturing. Some fibres are made to be intentionally birefringent. These are called polarisation maintaining (PM) fibres and are used in fibre interferometers, fibre optic sensing and quantum key distribution systems. Two common geometries are shown in Figure 2.27.

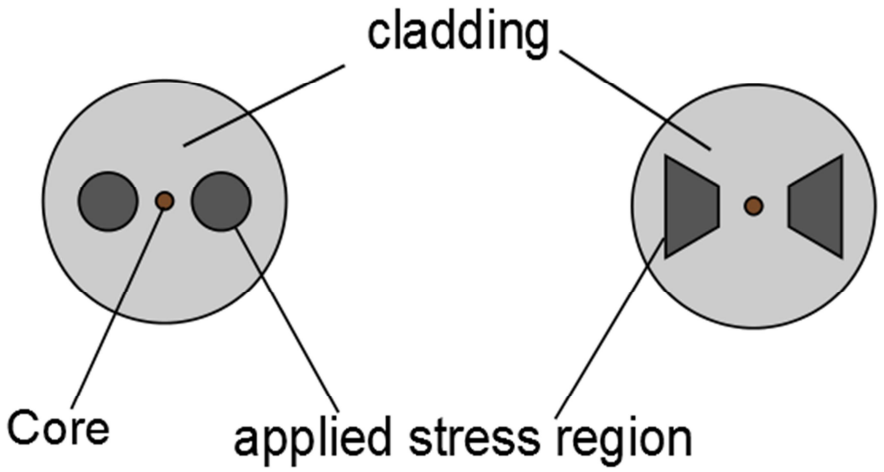

Figure 2.27. Design of two common PM fibres, on the left Panda and on the right bow-tie [107].

PM fibre maintains the existing polarisation of linearly-polarised light that is launched into the fibre with the correct orientation. If the polarisation of the input light is not aligned with the stress direction in the fibre, the output will vary between linear and circular polarisation. The exact polarisation will then be sensitive to variations in temperature and stress in the fibre [104], [106]. The ability of a PM fibre to preserve the state of polarisation is given by its beat length

$$L_b = \frac{2\pi}{\beta_x - \beta_y} = \frac{\lambda_0}{n_{eff}} \qquad \text{Equation (2.30)}$$

where β_x and β_y are the propagation constants along the x and y axis, n_{eff} is the effective refractive index and λ_0 is the wavelength. A low value of L_b corresponds to a fibre with a high polarisation preserving ability. The length L_b is the distance along the fibre in which the phase difference between the two orthogonal modes becomes 2π.

Light coupled into both fundamental modes of the fibre will repeat its state of polarisation every L_b as shown in Figure 2.28.

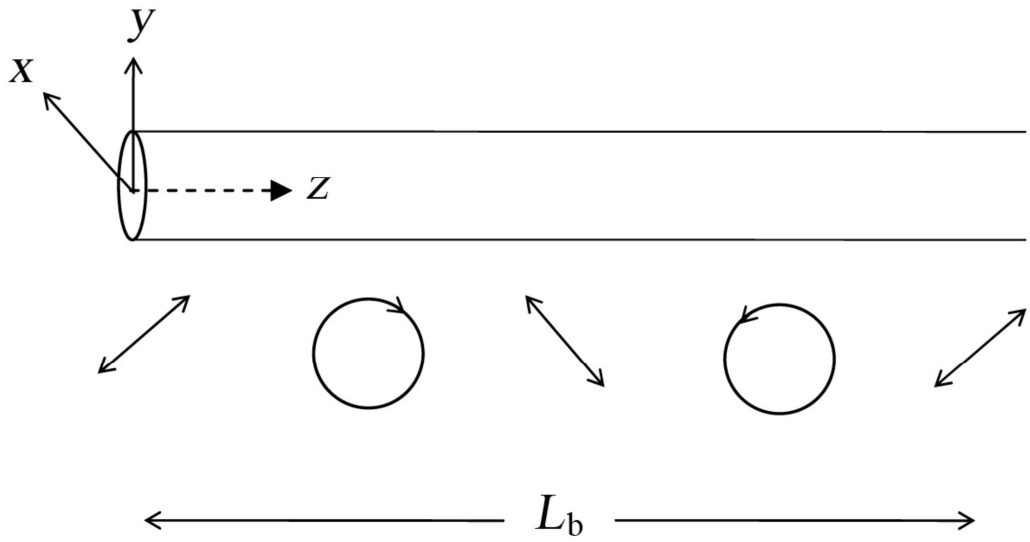

Figure 2.28. Evolution of the polarisation state of light guided along a birefringent fibre when the x and y polarised modes are equally excited [107].

2.10.1.2 Polarisation mode dispersion (PMD) and loss (PDL)

Polarisation mode dispersion is a fundamental property of optical fibres and it is the broadening of the input pulse due to a phase delay between the input polarisation states. A single mode optical fibre supports one fundamental mode which consists of two orthogonal polarisation modes. In an ideal case the core of the optical fibre is isotropic and both modes experience the same refractive index. However in real fibre due to birefringence affects each mode experiences a slightly different refractive index and travel with different group velocities. This means that a single input pulse launched into the fibre can split into orthogonally polarised pulses with each one having a different transit time shown in Figure 2.29. This effect can limit the bit rate of the communication system when dealing with ultra-fast communications [107]. The effect of PMD grows with the square root of the distance of the fibre and typical values for modern telecommunications fibres are 0.1 ps km^{-1}.

A closely related issue is polarisation dependent loss, which is the reduction in energy of the propagating light pulse that is preferential to one polarisation state. This differential loss can have the effect of changing the state of polarisation of the output beam. This can be an issue when trying to achieve high fringe visibilities with fibre interferometers.

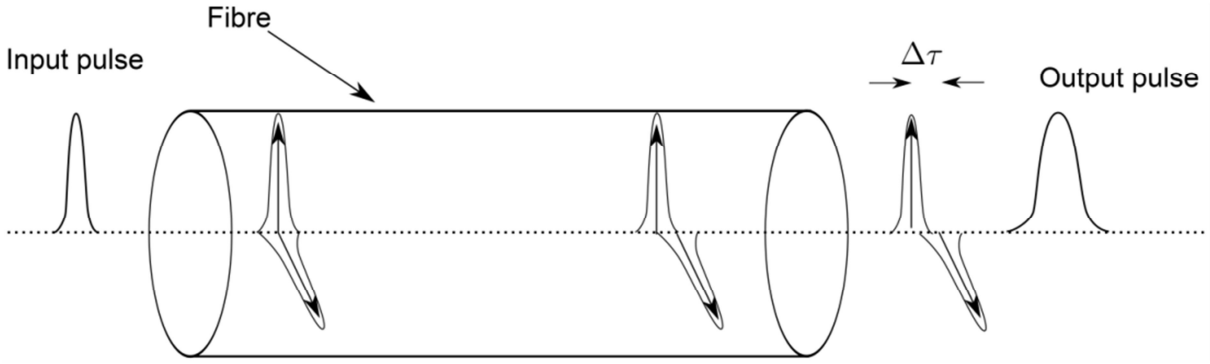

Figure 2.29. Polarisation mode dispersion (PMD) in optical fibres [107]. A short optical input into the fibre is temporally broadened as it propagates through the fibre by PMD.

2.10.1.3 Raman scattering

To ensure efficient use of resources it is beneficial if the quantum and classical channel can be shared on the same link as modern telecommunications. However this is limited by Raman scattering. Raman scattering is an inelastic scattering process in which scattered photons either gain (anti-Stokes) or lose energy (Stokes scattering) from interacting with a material. This is in contrast to Rayleigh scattering in which the energy of the photon remains unchanged upon scattering. Raman scattering is generated symmetrically in the forward and reverse directions in fibre and has a spectral width of up to 300 nm centered on 1550 nm [108]. Figure 2.30 shows a typical Raman spectra from an upstream and downstream laser centred at a wavelength of 1310 nm and 1550 nm respectively in standard telecommunications fibre.

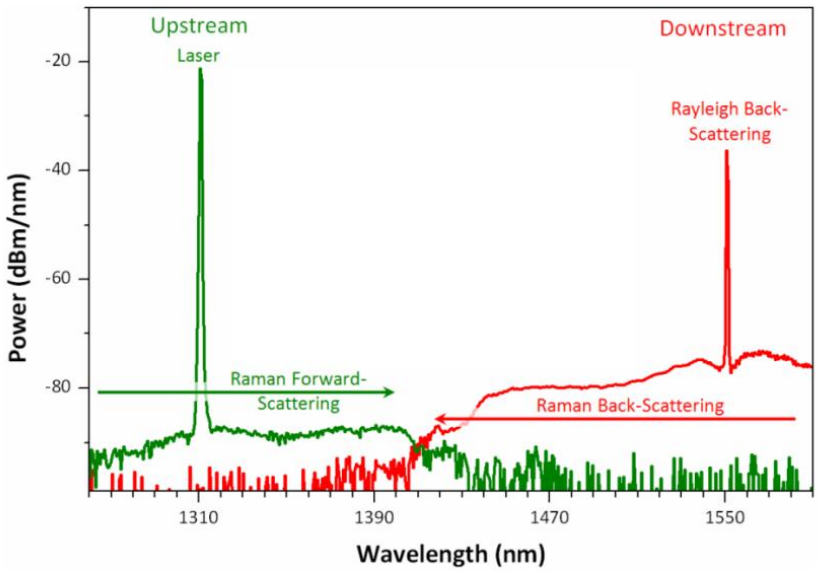

Figure 2.30. Raman scattering effect showing a broad spectrum from the upstream and downstream lasers used in classical communication systems [109].

Some of the photons travelling in the classical channel can undergo this Raman scattering and make its way into the quantum channel. Since classical channel power levels are ~10^7 orders of magnitude more powerful than quantum power levels Raman scattering can increase the error rate in the quantum channel [110]. This is particularly an issue with "*plug-and-play*" systems when Bob initials key generation by sending a bright light pulse to Alice.

2.10.2 Free space communication

Using free space as the quantum channel has many benefits for QKD applications over fibre. The atmosphere has a high transmission window at about 770 nm where single-photons can be detected using commercially available single-photon detectors with high efficiencies. The atmosphere is also a non-birefringent media at these wavelengths which means the polarisation of photons is preserved in transit. However there are also a few drawbacks to using free-space communication. Background from sunlight can increase the error rate and must be removed by spectral and spatial filtering. The effect of beam divergence is also a problem. Even using diffraction limited optics a 20 cm diameter beam at launch will expand to about 100 m after 300 km. This requires larger optics to ensure high collection efficiencies. Atmospheric turbulence can affect the arrival time of a photon and beam divergence but can be compensated for by using adaptive optics or using a reference pulse [17].

2.11 Single-photon detection

As previously discussed they are several technologies available for the generation of single-photons. In a QKD system it must also be possible to detect the light signal which has travelled through the quantum channel. These detectors must be sensitive to single-photons incident on the device. The primary detector technologies which have been used include semiconductor avalanche photodiodes, superconducting detectors and photomultiplier tubes. The single-photon detection efficiencies of some of these detectors are shown in Figure 2.31. When describing optical detectors it is useful to define some terminology to characterise them, namely detector efficiency, noise equivalent power, timing jitter, dark count rate and afterpulsing. The quantum efficiency of a detector is the probability that when an incident photon is absorbed it creates a detectable output electrical pulse. The noise equivalent power is a measure of the sensitivity of the detector and is defined as the signal power that gives a unity signal-to-noise ratio in a one hertz output bandwidth and is given by

$$NEP = \frac{h\nu}{\eta}\sqrt{2R} \qquad \text{Equation (2.31)}$$

where R is the count rate ,η is the detection efficiency, h is Planks constant and ν is the frequency. Dark counts are carriers created in the device which are uncorrelated with incident photons and can be caused by the thermal generation of carriers.

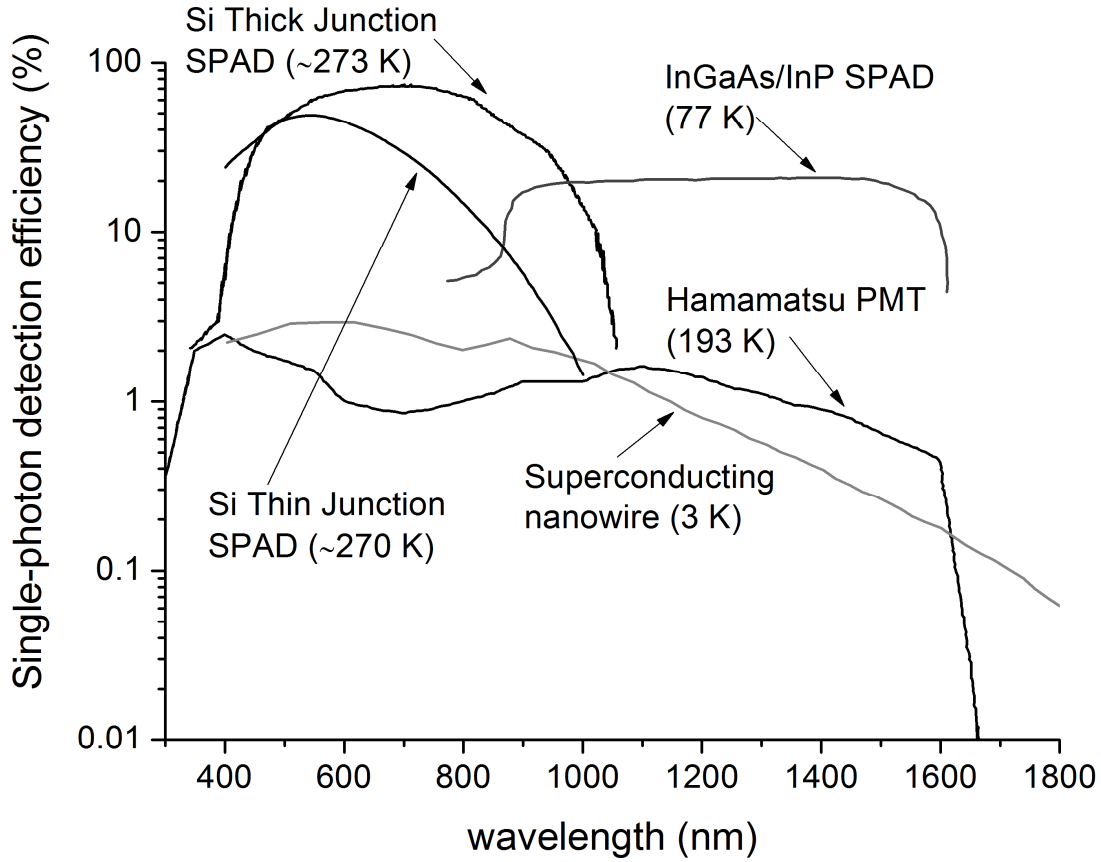

Figure 2.31. Typical single-photon detection efficiencies for silicon thin and thin junction SPADs, InGaAs/InP SPADs, photomultiplier tubes and superconducting nanowire detector technologies [111].

2.11.1 Single-photon avalanche photodiode (SPAD)

Single-photon avalanche photodiodes (SPADs) are p-n junctions that operate at reverse bias above the breakdown voltage. In this mode a single carrier can trigger a self-sustaining avalanche current. When a p-n junction is formed in a semiconductor material a region which is depleted of mobile charge carriers is created. An electric field appears across this depletion due to the presence of immobile atoms as shown Figure 2.32.

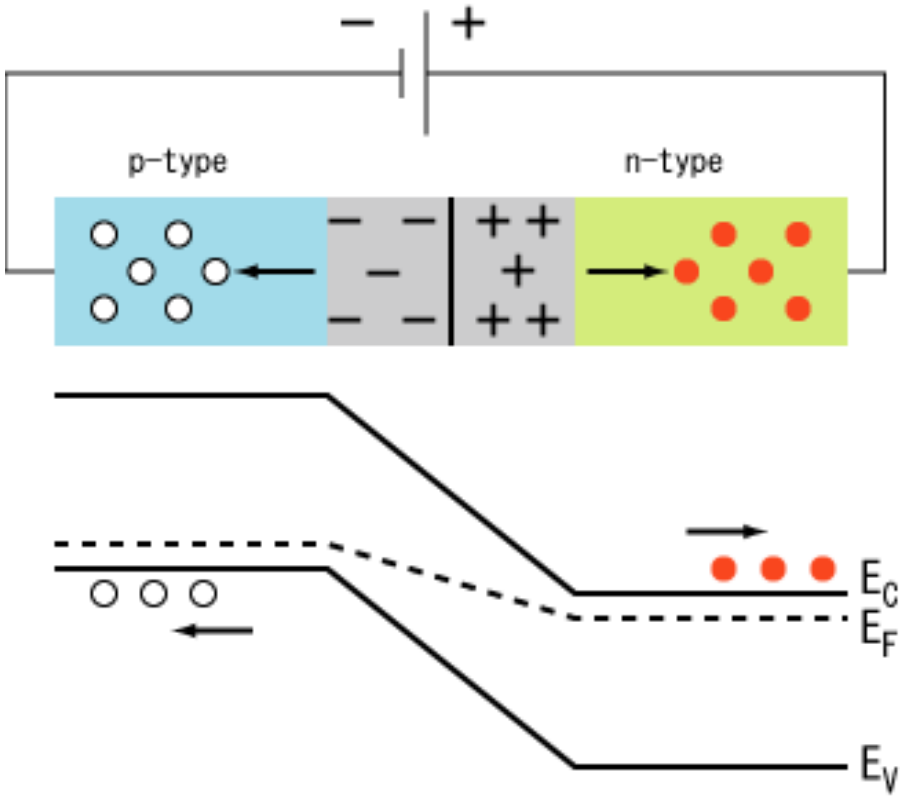

Figure 2.32. Energy bandgap of semiconductor p-n junction in reverse bias. The grey region indicates the depletion region which is devoid of mobile carriers.

If an electron-hole pair is generated in the depletion region by the absorption of a photon the carriers are separated by the electric field. The charge separation can be detected by reverse biasing the structure and measuring the current in an external circuit. Avalanche photodiodes work in a similar manner although they have internal gain built in for the amplification of the photocurrent. The current-voltage characteristic of an APD depends on the region in which it is biased as shown in Figure 2.33. In region I the device is forward biased and can be operated in the photovoltaic mode. In region II the device is reversed biased. When there is no illumination a dark current is observed due to thermally generated electron-hole pairs and also due to reverse bias leakage currents. When light is incident electron-hole pairs are created in the depletion region and swept out due to the electric field. An increase in the current is observed depending on the illumination level. In region III the device is biased close to but below breakdown voltage of the semiconductor. The high field results in photo-generated carriers undergoing impact ionisation and creating secondary carriers. The avalanche current in this region is directly proportion to the input illumination but without single-photon sensitivity. Most long-haul communication APDs are operated in this region.

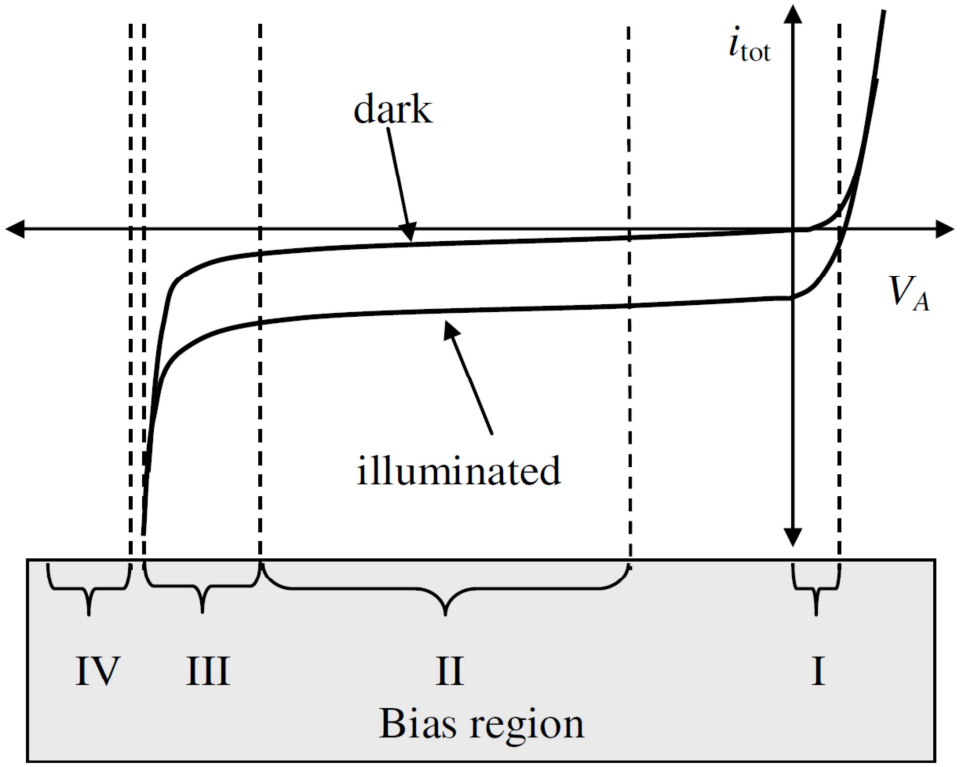

Figure 2.33 The current voltage characteristic of an APD structure under various biasing conditions [112]. Region I is forward biased and can be operated in photovoltaic mode. Region II is operated in reversed bias. When light is incident on the device in this mode of operation, electron-hole pairs are created in the depletion region. The current depends on the illumination intensity. Region III is biased close to but below the breakdown voltage. The high filed in this region results in photo-generated carriers undergoing impact ionisation creating secondary carriers. Most long-haul communication APDs operate in this region where the avalanche current is directly proportional to the illumination, but without single-photon sensitivity. Region IV is biased high under reverse bias and carriers can undergo impaction ionisation. There is a runaway avalanche process, where the gain is effectively infinite. The APD can have single-photon sensitivity in this regime.

In region IV the p-n structure is biased under high reverse bias voltages above breakdown. Carriers which travel through the depletion region gain enough energy to enable further carriers to be excited across the energy gap by impact ionisation shown in Figure 2.34. The current rises rapidly to a macroscopic level in a few nanoseconds. If the carrier is photo-generated, then the leading edge of the pulse marks the arrival time of the photon. The current continues to flow until the avalanche current can be quenched by reducing the bias voltage below the breakdown voltage. For another photon to be detected the bias voltage is then restored. A quenching circuit is needed

for this purpose which must be able to sense the leading edge of the avalanche current, generate an output electrical pulse, quench the avalanche current by lowering the voltage to the breakdown voltage and then restore the photodiode voltage to the operating level.

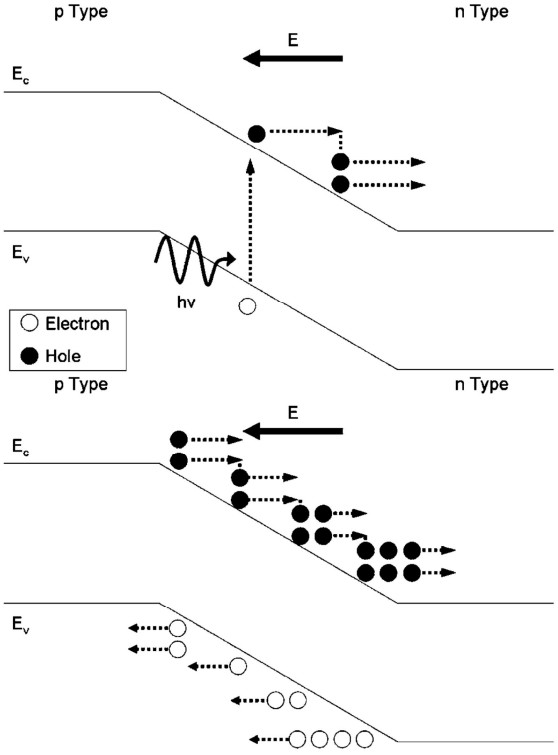

Figure 2.34. Impact ionisation process in an avalanche photodiode. An incident photon creates an electron-hole pair in the depletion region. Due to the high electric field in this region further carriers are created by impact ionisation and grows exponentially until a detectable current flows in the device [111].

2.11.2 Quenching circuits

When an APD is biased beyond its breakdown voltage a photo-generated events causes an avalanche process which needs to be stopped before the next photo event can be detected. There are primarily three different quenching methods currently used which are passive quenching, active quenching and gated quenching.

2.11.2.1 Passive quenching

Passive quenching, in which the avalanche circuit quenches itself, is the simplest form of quenching the avalanche process. This is achieved by biasing the device above the break down voltage with a series resistor typically with a resistance of several hundred kΩs, as shown in Figure 2.35. When the device is ready to detect a photon there is no current flowing. When a photo-generated event occurs, a high avalanche current flows through the device and reduces the voltage below the breakdown voltage thereby

stopping the avalanche process. The recovery time of the device is limited by the biasing resistance and the capacitance of the device [113].

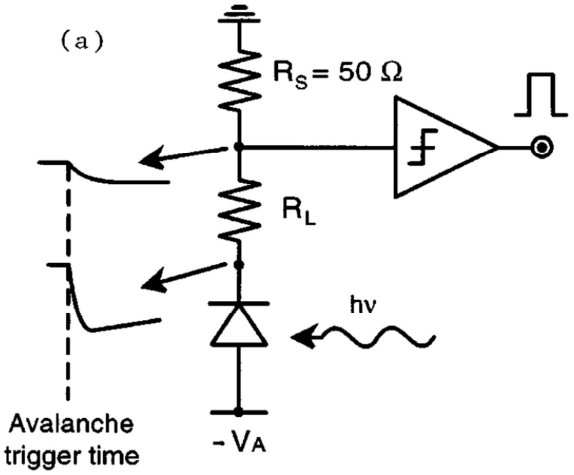

Figure 2.35. Schematic of the circuit arrangement for passive quenching [113]. Device is biased above breakdown by R_s and the avalanche current discharges through R_L.

2.11.2.2 Active quenching

Active quenching relies on the ability to detect the rise of an avalanche pulse and then control the reverse bias voltage. The quenching circuit shown in Figure 2.36 is able to sense the rise of the avalanche pulse by a fast comparator and switches the bias voltage source below the break down voltage. After a specific time called the hold-off time the bias voltage is again switched back to its original voltage. With active quenching the device can be quickly changed from Geiger mode to quenched mode and the small avalanche pulse limits the current through the device which improves after pulsing effects. This circuit is used extensively in commercially available Si SPADs [113].

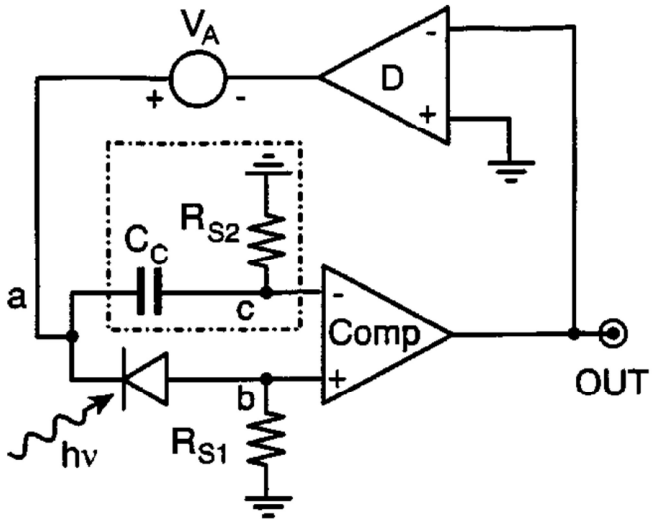

Figure 2.36. Schematic of the active quenching circuit [113].Comp is the comparator and D is the quenching and reset driver.

2.11.2.3 Gated quenching

For some single-photon detectors to avoid excessive problems with darks counts and afterpulsing effects it is necessary to operate the device in gated Geiger mode. Most InGaAs/InP detectors are gated in this manner. The device is biased a few volts below its breakdown voltage by a DC voltage. A gated pulse is superimposed onto the DC level which means that the device only operates in Geiger mode for the duration of the gate pulse. This form of gating is useful when the arrival time of a photon is well defined like in time-of-flight laser range finding and QKD. A schematic circuit diagram for gated quenching is shown in Figure 2.37.

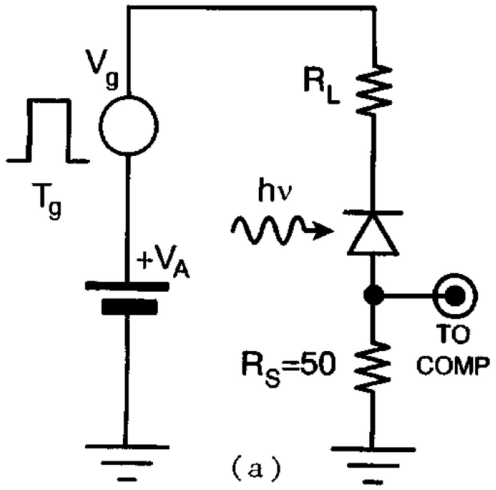

Figure 2.37. Schematic of the circuit for gated quenching [113]. V_g is the voltage generator of the gating signal of time duration T_g.

2.11.3 SPAD electrical timing jitter

The electrical timing jitter of a single-photon avalanche diode, which is the variation in delay between the absorption of a photon and the generation of an output electrical pulse, can depend on many processes including the depth of the photon absorption which leads to variations in the drift time [114] and also the stochastic nature in which carriers are generated in the multiplication process [115]. The typical response of a SPAD is shown in Figure 2.38. It is characterised by a fast peak and a slow tail. The peak is caused by the photo-generated carriers within the depletion layer of the active junction. The width of the peak is determined by the stochastic nature of the avalanche build-up time and the timing resolution can be improved by increasing the maximum electric field in the active junction. The tail is due to the carriers photo-generated in the neutral region beneath the junction and reach the depletion region by diffusion [114].

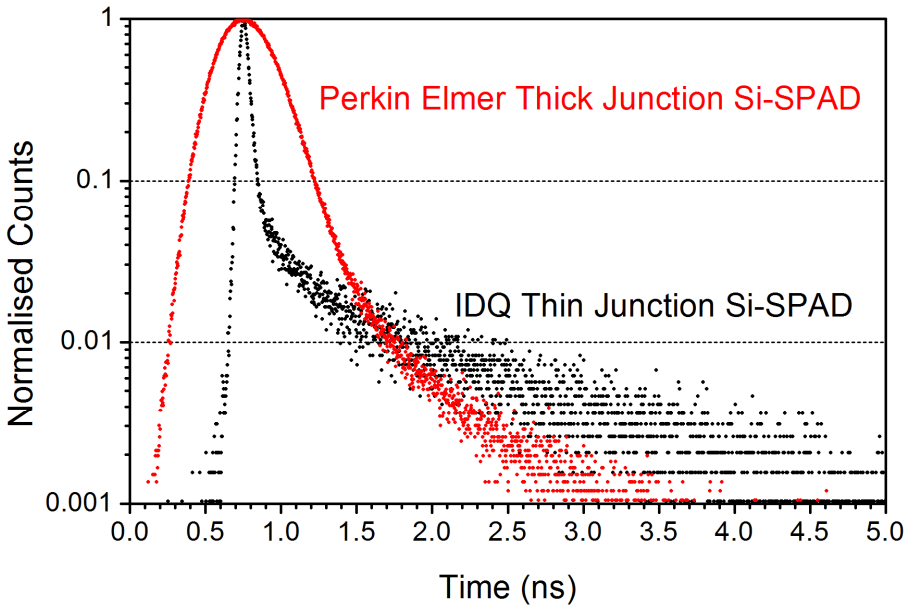

Figure 2.38 Typical instrumental response of a thick and thin junction Si-SPAD [116].

2.11.4 Thick and thin junction Si-SPADs

Silicon SPADs can be divided into two main groups depending on the thickness of the depletion layer of the p-n junction; thin junction diodes are typically a few µm and thick junction devices are typically 20-200 µm. Thin depletion layer SPADs (Figure 2.40) can be characterised by a breakdown voltage of 10-20 V, small active region area with a diameter from 5 µm to 100 µm, photon detection efficiencies from 45% at 500 nm to about 10% at 820 nm and very high resolution in photon counting, better than 100 ps FWHM and better than 30 ps with a small active region [114], [117], [118]. Reachthrough SPADs with thick depletion layer (Figure 2.39) have a breakdown voltage from 200–500 V, detection efficiency of over 50% in the wavelength window of 540-850 nm and a timing resolution of 350 ps FWHM [119], [120], [121].

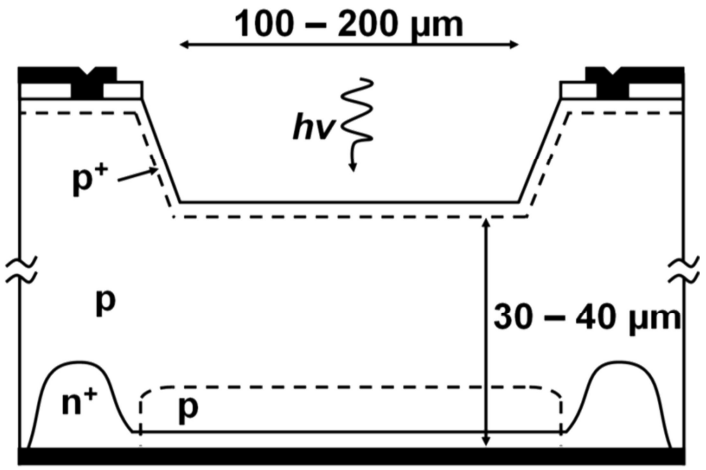

Figure 2.39 Geometry of a thick junction Si-SPAD [111].

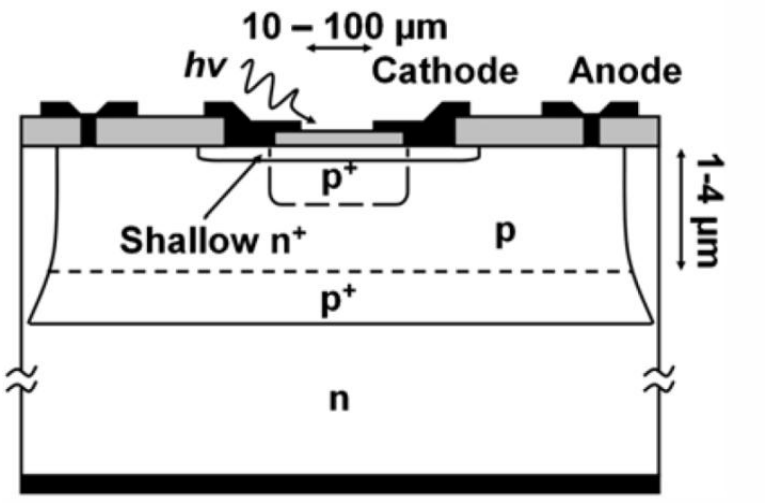

Figure 2.40 Geometry of a thin junction Si-SPAD [111].

Due to the spectral responsively of silicon, SPADs based on this material have relatively poor quantum efficiencies at the telecommunications band around 1310 and 1550 nm wavelength as seen in Figure 2.31. To improve the performance of SPADs at these wavelengths it is necessary to use a material with a suitable narrow bandgap like Ge or InGaAs. These devices use separate absorption (InGaAs) and gain medium regions (InP) and are based on the heterojunction between InP and InGaAs (Figure 2.41). Under reverse bias operation, a high electric field is large enough to induce impact ionisation in the InP layer, which is the multiplication layer of the device. Long wavelength photons incident on the device pass through the InP layer and are absorbed in the narrower bandgap layer producing electron-hole pairs. The device is designed so that under normal operating conditions the depletion region extends from the p^+n junction in the InP layer into the InGaAs layer. Photo-generated carriers created in the InGaAs layer will undergo drift because of the presence of the electric field. In order to obtain low multiplication noise the carrier with the higher impact ionisation coefficient should initiate the avalanche process.

The valence band discontinuity between the InP and the InGaAs layers hinders the transportation of holes from the narrow gap InGaAs material to the wider gap InP material. To increase the transport of holes, a quaternary layer of InGaAsP is placed between the InGaAs and the InP layers, a schematic of which is shown in Figure 2.41. The layer of InGaAsP has an intermediate bandgap between that of the InP and the InGaAs and grades the valence band discontinuity. The result of this is that holes can cross the barrier more efficiently. Due to dark counts and after-pulsing effects these

devices were found to operate best in gated Geiger mode using a periodic gate signal but have also been demonstrated using the passive quenching method but still suffered from high dark count rates of several hundred kHz [122]. The gating frequency was initially limited to several hundred kHz but now using a self-differencing circuit an InGaAs device has been operated at up to 2 GHz with a QE of 11.8 % at telecoms wavelengths [123].

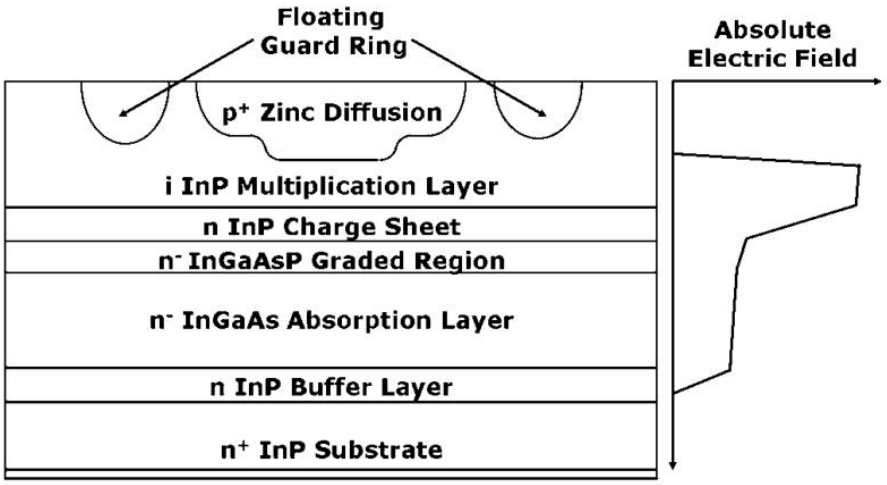

Figure 2.41. Cross-section of an InGaAs/InP SPAD structure and absolute electric field (right) [124].

2.11.5 Afterpulsing and trapping centres

If one of the carriers trapped from previous avalanche pulses are released when the bias is again above the bias voltage that carrier may succeed in triggering further avalanches. This effect is known as afterpulsing and contributes to the overall dark count rate of the detector. The presence of trapping centres depends on the quality of the material used in the detector. Afterpulsing from trapping centres are often thought to be located in the high-field region of the junction where impact ionisation occurs [124]. This is a low temperature effect because the emission lifetime of carriers from trapping levels grows exponentially with decreasing temperature. A compromise is often needed between the count created by thermally created carriers and those created by afterpulsing. At low temperatures the dark count rate is reduced but the trapped carriers have a long lifetime and afterpulsing effects are even seen at relatively low count rates of a few kHz. This effect is especially seen in Ge and InGaAs/InP APDs. The afterpulsing probability is directly proportional to the amount of current flowing through the device and techniques which limit the current flowing through the device can decrease this probability [125].

2.11.6 Cavity enhanced single-photon detectors

All photon counting applications would benefit from increased detection efficiencies. In the case of SPADs the easiest way of achieving this would be to increase the depletion region thickness. However the high electric field strength across the depletion region would require high operating voltages leading to heating effects. An increased depletion region would also increase the timing jitter due to photon absorption in neutral regions creating minority carriers which then diffuse into the depletion region [126]. The probability of a photon being absorbed can be increased by the use of a Fabry-Pérot cavity which increases the optical field inside the cavity at resonant frequencies [127]. A planar SPAD device can be grown between two reflectors as shown in Figure 2.42.

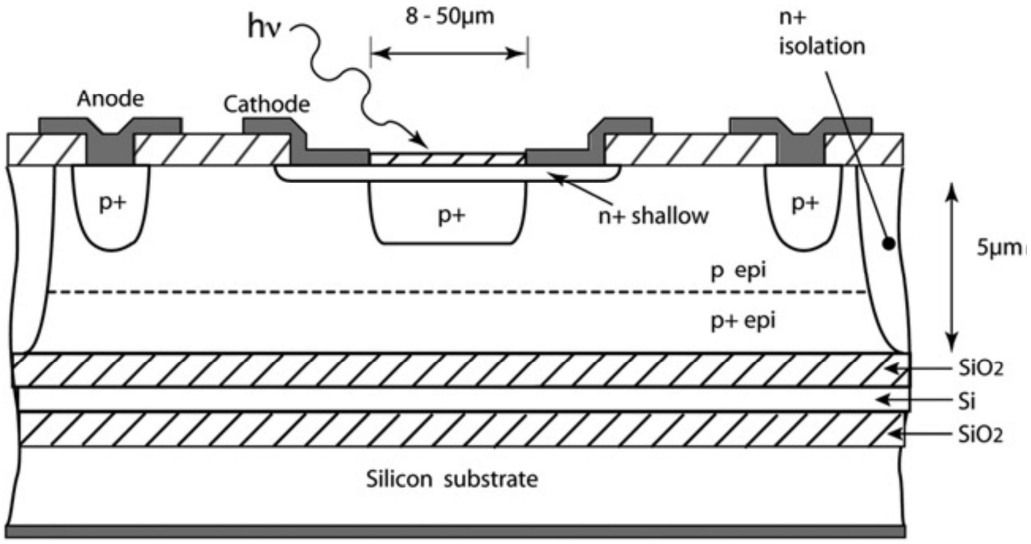

Figure 2.42. Schematic of the cross section of a resonant cavity SPAD [128]. The cavity is formed by the buried Bragg reflector and the air interface at the surface.

The lower reflector uses a two-period distributed Bragg reflector fabricated using commercially available silicon-on-insulator process (SOI). The thickness of the DBR layers (437 nm for the SiO_2 layers and 174 nm for the Si layers) was specifically tuned to achieve a reflectance in excess of 90% around 850 nm. The SPADs are then grown on top of this reflecting wafer. The top reflector is provided by the upper semiconductor air interface. The detection efficiency of the device reported by Ghioni *et al.* was about 34% at a wavelength of 850 nm shown in Figure 2.43 with a photon timing resolution less than 35 ps full-width at half-maximum [128].

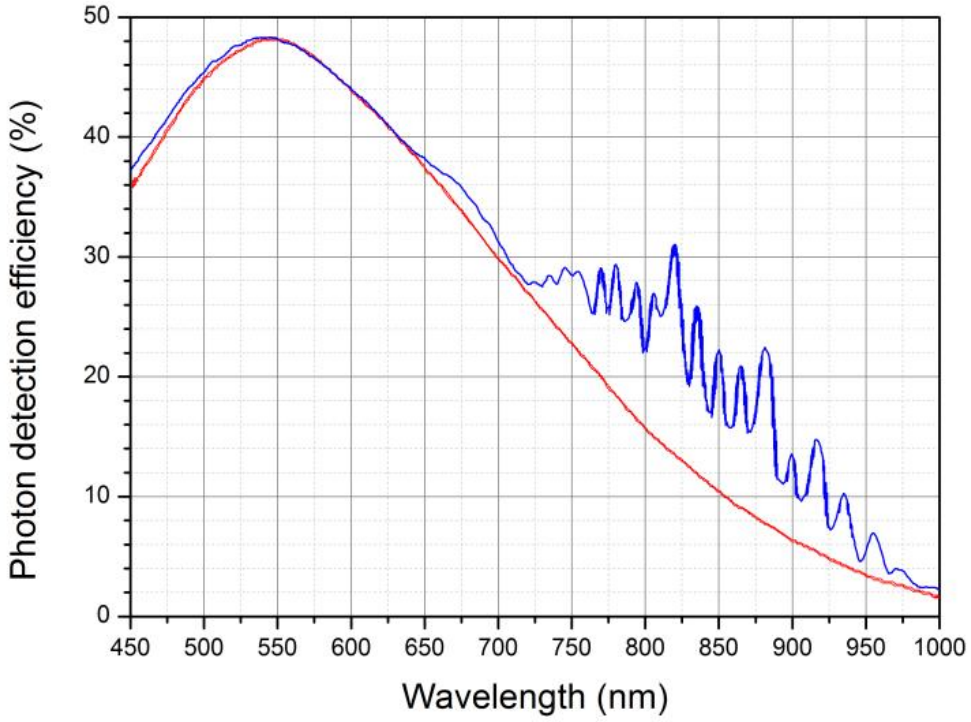

Figure 2.43. Detection efficiency for control SPAD (red) and the resonator cavity enhanced SPAD detector (blue) [128].

2.11.7 Transition edge sensors (TES)

Superconducting transition edge sensors operate on the principle of a bolometer in which the absorption of a photon energy is detected as a rise in temperature. A bolometer typically consists of an absorber and a thermometer of heat capacity C which is connected by a small thermal conductance G, to a heat sink held at a fixed temperature shown in Figure 2.44. The energy E of the incident radiation is converted into heat in the absorber, leading to a temperature rise, until the radiation power flowing into the absorber is equal to the power flowing into the heat sink through the weak thermal link. The temperature rise is subsequently measured and is directly proportional to the absorbed energy [129]. The fine temperature sensitivity which is required for single-photon detection is obtained by a thin film of superconducting material which is in transition between superconducting and normal resistance on an insulating substrate. A constant bias is applied across the film which increases the temperature of the electrons above that of the substrate. When a photon is absorbed the increase in the temperature in the sensor increases its resistance which then reduces the current flowing through it, thereby reducing the heating effect caused by ohmic heating. The temperature is maintained at a constant level by the constant bias voltage in addition to the negative feedback from the reduction in the ohmic heating. A single-photon can be detected by the reduction in the current flowing in the sensor [130].

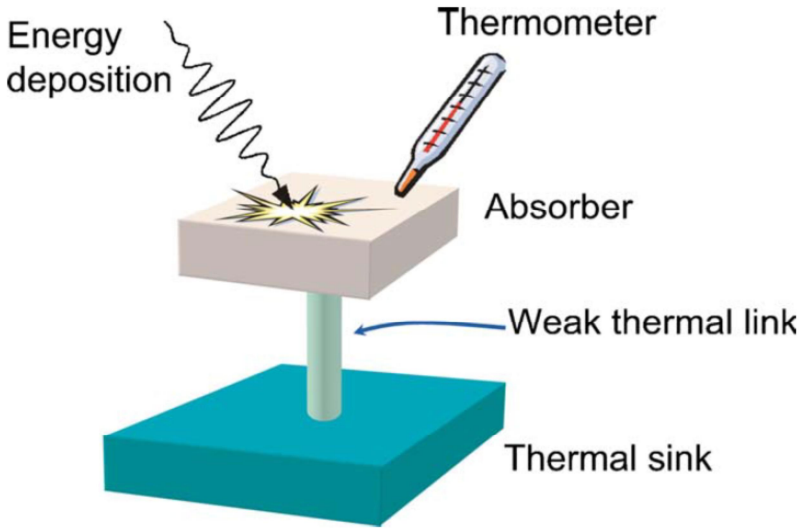

Figure 2.44 Schematic of a transition edge sensor. A bias voltage keeps the electrons in the absorber between superconducting and normal resistance. The absorption of a photon increases the temperature of the sensor and increases the resistance of the device. The reduction in current signifies the detection of a single-photon [131].

Although not implementing single-photon detection, superconducting TES are currently being used as one of the sensors for the European Space Agency's James Clark Maxwell telescope in Mauna Kea Observatory, Hawaii [132]. The SCUAB-2 camera (sub-millimetre common user bolometer array) is designed to operate in the sub-millimetre wavelength regime where it is particularly sensitive to electromagnetic emission from interstellar dust and gas which is of interest to studying stellar and planetary evolution [133]. Simultaneous measurements are performed at wavelengths of 450 μm and 850 μm. As is common with most bolometers, thermometry and absorption are performed by different materials. The absorber is a doped silicon surface and the heat is coupled though to the TES [129]. Observations in the sub-millimetre band are used to trace molecular (H_2) gas clouds in galaxies, using spectral emission lines from trace molecules or the continuum thermal emission from dust grains.

2.11.7.1 Superconducting nanowires

Superconducting devices are becoming a very attractive radiation sensor because of their ultrafast response and quantum nature. Each absorbed photon is able to generate a large number of excited particles because the superconducting energy gap 2Δ, is 2-3 orders of magnitude lower than the bandgap in most semiconductors which create efficient secondary electron cascade. Their operation can be followed using Figure 2.45.

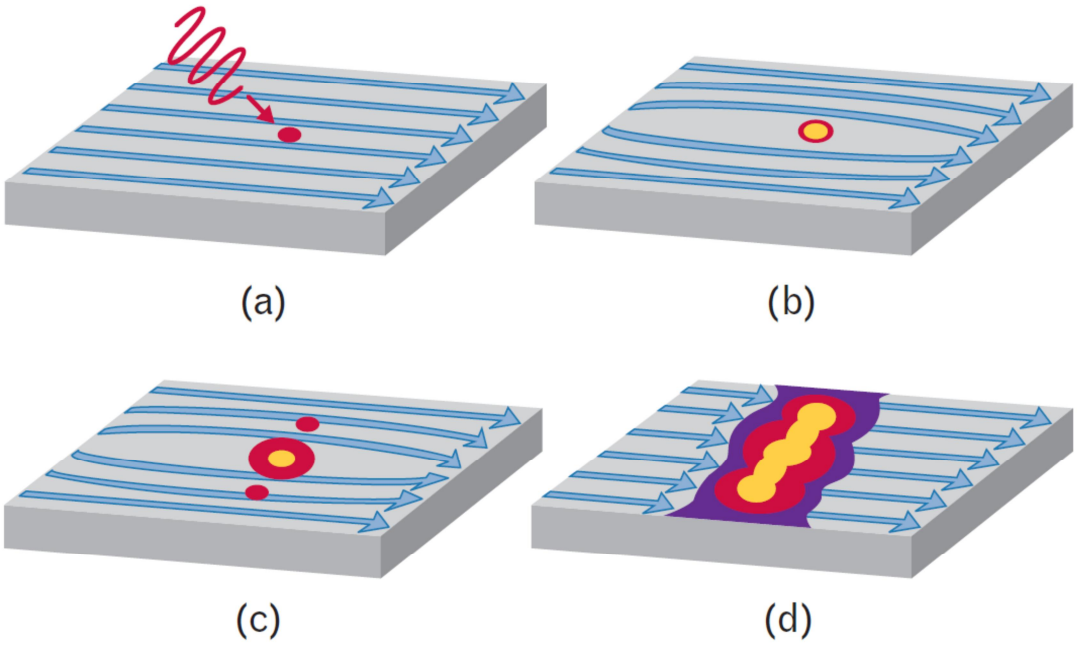

Figure 2.45 (a) The absorption of a photon creates a resistance hotspot region within the nanowire. (b)The superconducting current is expelled from the resistive hotspot, increasing the current density in the adjacent areas of the nanowire. (c) the superconducting biasing current is exceeded in the sidewalks (d) a non-superconducting barrier is formed across the entire width which results in a voltage signal [134].

When a photon of light $h\nu$ is absorbed by a Cooper pair, highly excited quasiparticles are created. A Cooper pair is composed of two electrons which are bound together at low temperatures [135]. These particles lose their energy on a very fast time scale of ~10 fs by electron-electron scattering and by the creation of an avalanche of secondary quasiparticles. At lower energies these excited quasiparticles lose their energy by electron-phonon interaction. The mean free path of these phonons is small and they break other Cooper pairs. As the average energy of the excited electrons in the cascade decreases toward the energy gap 2Δ, their number increases reaching $h\nu/2\Delta$ and their effective temperature T_c increases above the superconducting critical temperature. The result is that a single-photon can create the collapse of superconducting in a localised region and the formation of a normal-state hotspot region. The hotspot formation enables a precise detection of the photon arrival event. When a localised hotspot is created it grows due to the diffusion of quasiparticles out of the hotspot core. The biasing super current is prevented from flowing in the resistive hotspot volume and is instead concentrated near the edges of the film. The biasing current exceeds the critical value outside the hotspot and phase slip centres are created in the sidewalks. The

superconductivity is destroyed and a resistive barrier is formed across the entire cross-section of the stripe. The resistive barrier produces a voltage signal which is directly proportional to the biasing current. The hotspot then decreases in size due to relaxation and diffusion of the quasiparticles. After about 30 ps the hotspot stripe collapses and superconductivity is restored [136], [137], [134].

These type of detectors have been used in quantum key distribution systems demonstrated by Takesue *et al.* at the National Institute of Standards and Technology [62] and by Hadfield *et al.* in a 1550 nm fibre-based QKD link clocked at 3.3 MHz [138].

2.11.8 Photomultiplier tubes

Photomultiplier tubes (PMT) operate using the principle of the photoelectric effect. When light is incident on a photo-emission surface with a low work function electrons are emitted from the surface. These photoelectrons are then accelerated towards a series of electrodes called dynodes which are successively at higher potentials with respect to the cathode [96]. When an electron strikes the dynode it causes the emission of multiple secondary electrons which themselves are accelerated towards the next dynode and continues the multiplication process. These tubes must be operated in a vacuum to avoid electrons colliding with air molecules. A box-and-grid type PMT is shown in Figure 2.46.

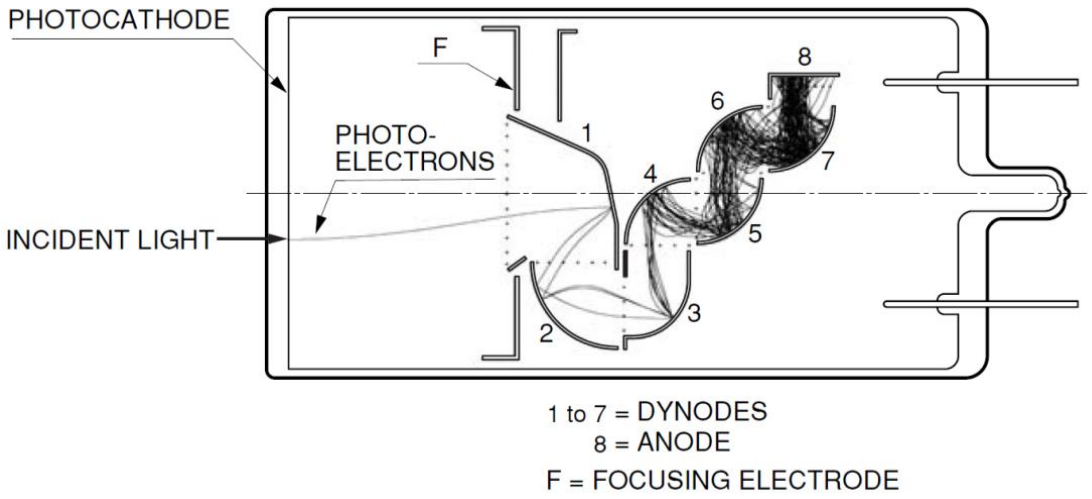

Figure 2.46 Box-and-grid type PMT [139]. The dynodes are labelled 1 to 7, the Anode is labelled 8 and F is the focusing electrode.

The wavelength of the PMTs maximum response and long wavelength cut-off is determined by the combination of the alkali metal that is used for the photocathode and its fabrication process. The spectral response of these devices can be extended up to 1.7 μm by using InP/InGaAs(Cs) as the photocathode material as shown in Figure 2.47.

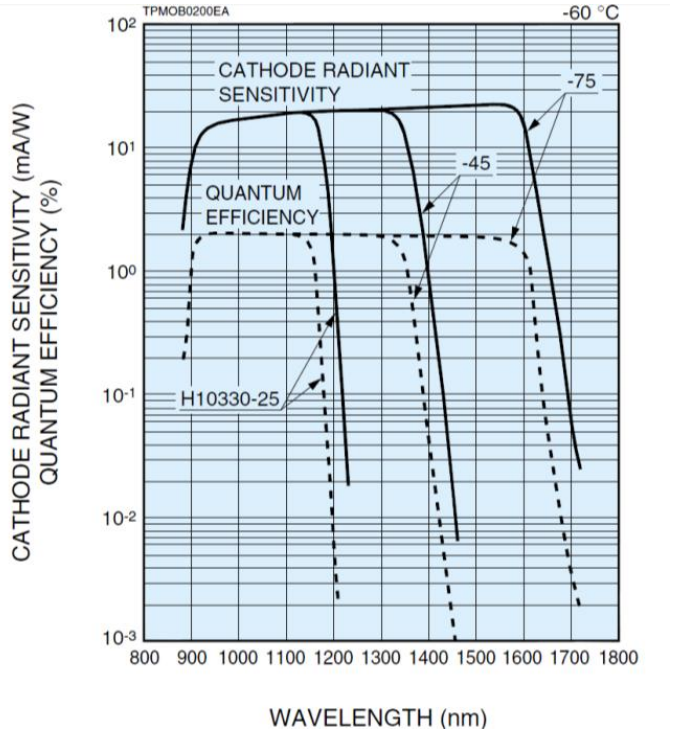

Figure 2.47 Quantum efficiency of three PMTs available from Hamamatsu [140]. The maximum quantum efficiency is about 2% for these devices.

The quantum efficiency of these devices is typically about 40% at a wavelength of 500 nm and 2% at 1550 nm [96]. The relatively large area of the device means that it is quite useful when collecting light from an extended source but has the disadvantage that the vacuum technology tends to make bulky devices which limits its reliability and scalability. The most common types are box-and-grid shown in Figure 2.46, ventain blind and linear focused. PMTs are capable of giving extremely high sensitivity and very fast response. PMT have a noise free gain on the order of a million however the timing jitter of such devices are limited to about 1 ns which means that they are unsuitable for applications such as gigahertz quantum key distribution systems [96].

2.11.9 Quantum dot field-effect transistor detectors

In 2000 Shields *et al.* demonstrated that the conductance of a field effect transistor (FET) gated by a layer of quantum dots was sensitive to the absorption of a single-photon. Unlike many traditional semiconductor single-photon detectors which depend

on the avalanche process, the gain in a quantum dot detector is achieved from the fact that the conductivity of the FET channel is very sensitive to the photo-excited charge trapped in the dots [141], [142]. The device shown in Figure 2.48 consists of a thin layer of quantum dots located between the gate electrode and conduction channel in a field-effect transistor (FET). Photo-generated carriers are captured by the dot and alter the channel conductance of the FET. The change in this conductance can be used to detect a single-photon. The quantum efficiency of these devices can be as much as 68% at a wavelength of 805 nm [142] but they suffer from larger timing jitters in the order of microseconds [143].

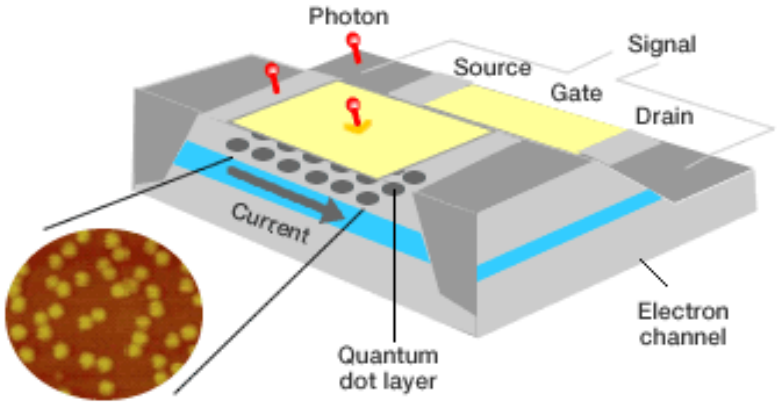

Figure 2.48 Diagram of a quantum dot FET. The quantum dots located between the gate electrode and conduction channel in a field-effect transistor [144].

2.11.9.1 Photon number resolving detectors

The ability to be able to resolve the number of photons in an optical pulse would be a considerable benefit to the field of quantum information where n-photon states are produced. In the past photon number resolving detectors were approximated using beam splitters and single-photon sensitive detectors but the probability of detecting N photons drops exponentially with N due to the probabilistic path a photon can take at a beam splitter even for 100% efficient detectors [131]. Recently, photon number resolving detectors have been demonstrated using transition edge sensors and also avalanche photodiodes using self-differencing technique. In TES detectors which are near the superconducting critical temperature a rapid change in resistance enables a very sensitive measurement of the temperature. This change in temperature is proportional to the photon energy which enables the sensor to be able to resolve the number of photons in a monochromatic optical pulse [131]. Superconducting nanowires have been shown to have photon number resolving capabilities when a series of nanowires are

connected in parallel and each connected to a series resistor. The linear addition of the currents on an external load from the different wires produces an output pulse which is proportional to the number of photons [145].

In 2008 Kardynał *et al.* demonstrated photon number resolving in avalanche photodiodes [146]. When InGaAs APDs are operated in gated Geiger mode, the output signal produced by a photo-induced electron-hole pair is affected by the capacitance response of the device to the gating signal pulse. To be able to resolve photon numbers it is necessary to measure the current shortly after the avalanche build up. The output signal is split into two paths one of which has a delay. They are then recombined with a difference circuit which removes the capacitance response of the device and the small current which is produced shortly after avalanche build up can be detected. The device then produces an avalanche current which is directly proportional to the incident photon flux.

2.11.10 Electron multiplying charge couple device (EMCCD)

Electron multiplying charge couple devices (EMCCD) are a digital camera technology that are able to detect single-photons while at the same time achieving high quantum efficiencies via an electron multiplying structure built into the sensor. This allows the use of the full quantum efficiency of the silicon sensor which can be as high as 95% using back illumination techniques. EMCCDs resemble traditional CCD cameras in use today in which the object is imaged onto a capacitor array in which it builds up an electric charge proportional to the light intensity. A control circuit then causes each capacitor to transfer its contents to its neighbour operating as a shift register. The last capacitor in the chain dumps the charge into a charge amplifier and converts it into a voltage. In EMCCD sensors the shift register is extended to include a gain register where weak signals can be detected above the readout noise of the camera at any readout speed. The gain register is similar to a shift register and consists of a line of electrodes which are driven by a controlled sequence of voltages to move charges to the next electrode in the chain. However in the gain register, one of the three voltage phases is a high voltage pulse typically 40-60 volts. This high electronic field can create secondary carriers through impact ionisation thereby creating gain [147]. EMCCD cameras are commercially available with a sensor size of 512×512 pixels (16×16 μm pixel size), a full frame rate of 56 per second and an overclocked readout of 17 MHz [148]. These types of cameras are particular useful in quantum imaging [149]

and continuous variables QKD protocols [28] where the spatial information of arriving photons is important.

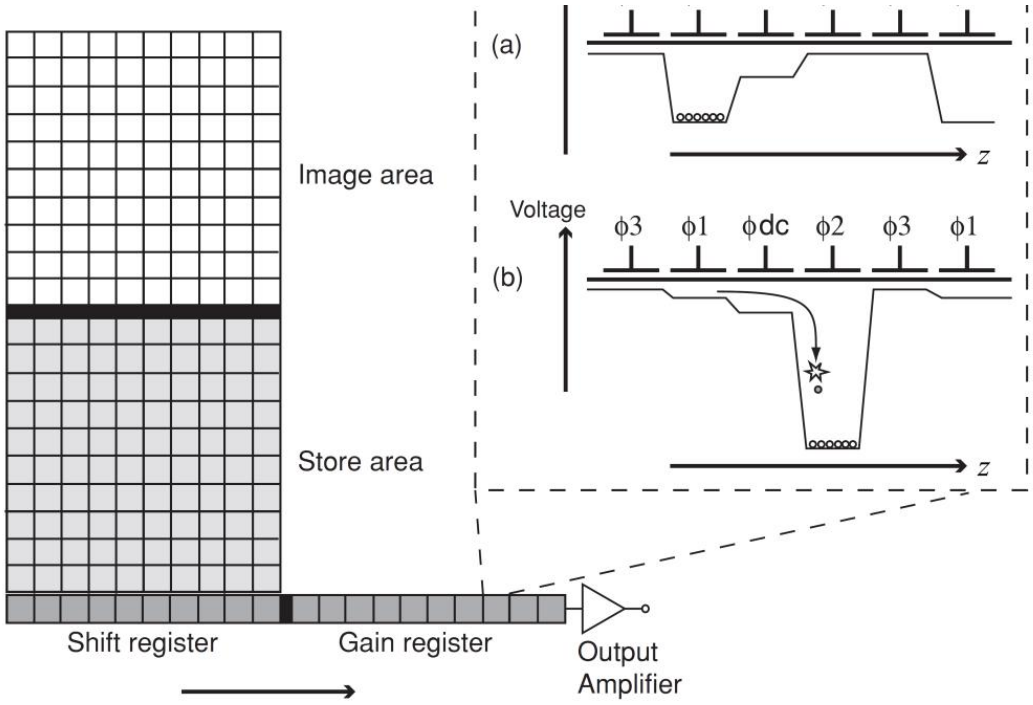

Figure 2.49. Schematic of EMCCD. Charges are transferred across the shift and gain register by a controlled sequence of voltage pulse. Gain is achieve by applying a large voltage at phase ϕ_2 causing avalanche multiplication via impact ionisation [147].

2.12 Time correlated single-photon counting techniques and counting modules

2.12.1 Time correlated single-photon counting

Time correlated single-photon counting (TCSPC) is a very sensitive method for recording repetitive low-light levels with high resolution and precision. It involves the detection of single-photons from a periodic light signal and using the detection time to reconstruct the waveform of the light pulse. It was originally designed to measure time-resolved fluorescence and photoluminescence. The TCSPC technique relies on the fact that when using low light signals, the probability of detecting one photon in a signal period is much less than one [150], [151], [152]. The TCSPC technique is in some ways analogous to a stop watch. The stop watch is started by a start signal which can be an external clock. The detection of a photon produces an electrical signal which is then used to stop the timer. The difference in time between the start and stop is then recorded. This is repeated many times and a histogram is produced of the time difference between the photon arrival times and the clock signal. The histogram which is produced is a representative of the original shape of the waveform.

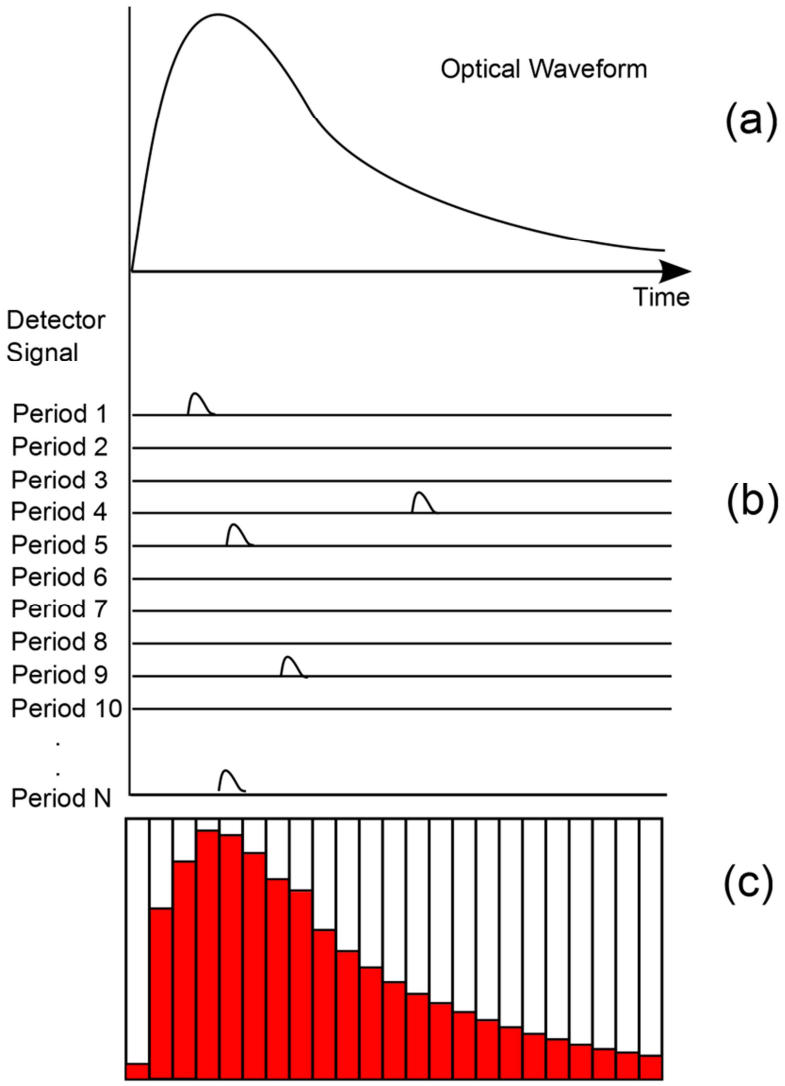

Figure 2.50.Principle of TCSPC [153]. (a) shows the input analogue signal, (b) shows the individual detector pulse from each clock period and (c) shows the resulting histogram.

Figure 2.50 shows the TCSPC technique in more detail. The detector signal is composed of a sequence of randomly distributed pulses which correspond to the detection of the individual photons. When a photon is detected, the time of the corresponding detector pulse in the signal period is measured. The events are collected in memory by adding a '1' in a memory location with an address proportional to the detection time. After many photons the distribution of the detection times, which is the waveform of the optical pulse, is built up. The time of the individual single-photon pulses can be measured with high precision [153]. Photon counting techniques offer several advantages over analogue techniques. The bandwidth of a photon counting experiment is only limited by the transit time spread of the pulses in the detector and not by the width of the single-photon pulses.

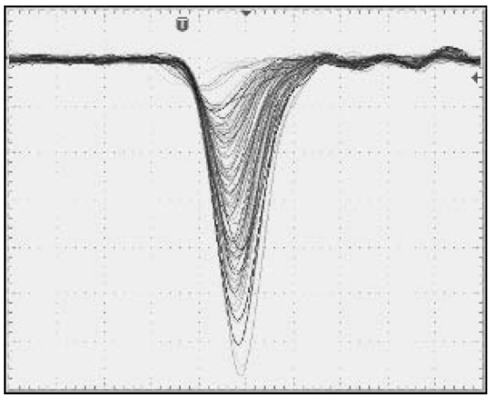

Figure 2.51. Typical electrical timing jitter from a detector showing a series of superimposed detector signals [153].

Single-photon pulses can suffer from considerable amplitude jitter. This amplitude or gain noise of the detector is a result of the random amplification process of the detector. A typical single-photon pulse obtained from a photomultiplier tube is shown in Figure 2.51. In analogue techniques the gain noise adds to the noise of the measurement. In TCSPC techniques the effect of amplitude jitter is removed by constant fraction triggering.

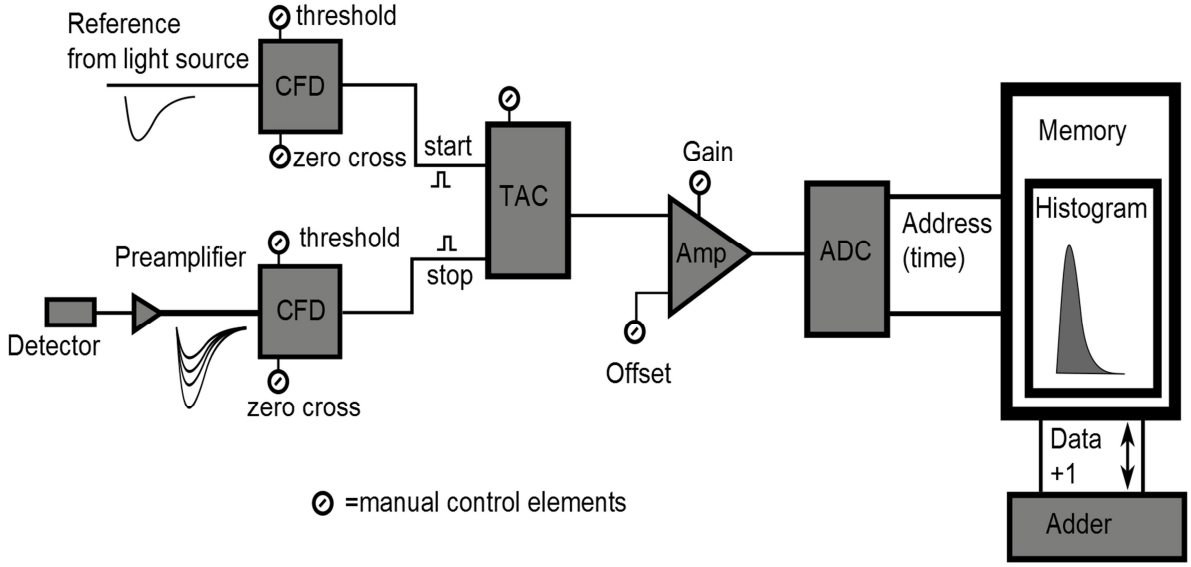

Figure 2.52 Architect of TCSPC module (forward mode) [153]. The CFD is the constant fraction discriminator, TAC is the time-to-amplitude converter, Amp is the amplifier and ADC is the analogue to digital converter.

The general architect of the TCSPC is shown Figure 2.52. The detector produces pulses from a periodic light signal which is then detected by a fast discriminator. The amplitude of these pulses fluctuates because of the varying gain of the detector. If a simple leading edge discriminator was used it would trigger when the leading edge of the pulse reached a certain threshold. This amplitude jitter would induce a timing jitter

which would be comparable to the pulse rise time. To overcome this issue a constant fraction discriminator (CFD) is used which triggers at a constant fraction of the pulse height.

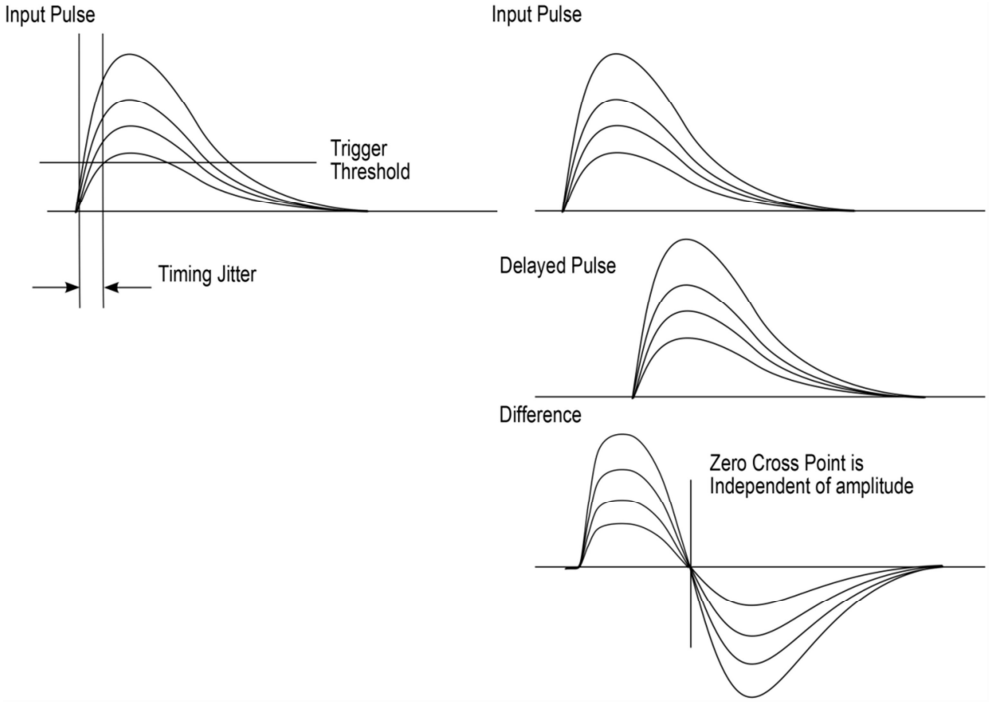

Figure 2.53 Left is a demonstration of the timing jitter caused by amplitude jitter. Right shows the method of constant fraction triggering [153].

Constant fraction triggering is achieved by triggering on the zero cross point of the sum of the input pulse with the delayed and inverted pulse as shown in Figure 2.53. The time position of the zero cross point is independent of the pulse amplitude and triggering on this point minimises the timing jitter induced by the amplitude jitter.

The time to amplitude converter (TAC) measures the time of a detected photon from the pulse at the detector input to the next pulse at the reference pulse. TCPSC modules like the Becker and Hickel SPC-600 operates in “reverse start stop”. In this mode the TAC is started when a photon is detected and is stopped with the next reference pulse. The “reverse start stop” method enables high photon count rates at high pulse repetition rates as it reduces the TAC trigger rate. When the TAC is started by a pulse at the start input, it generates a linear ramp voltage until a stop pulse appears at the stop input. In effect the TAC generates an output voltage depending linearly on the temporal position of the photons. The output from the TAC is then used as the input to a programmable gain amplifier. The gain can be changed which enables the user to select a smaller time window within the full-scale conversion range of the TAC. The SPC 600 can operate in two modes; histogram mode and in “time tag” or “FIFO” (first in, first out) mode. The

FIFO mode does not build up a photon distribution but stores information about each individual photon. For each photon the time in the signal period, the channel word, and the time from the start of the experiment (macro-time) is stored in a FIFO buffer. The FIFO buffer is continuously read during the course of the experiment and the photon data is stored in memory. The benefit of the "FIFO" mode over the histogram mode is that it gives timing information for each individual photon. There are two clocks recording the arrival times of photons, one called the macrotime clock records the time since the start of the experiment and the microtime clock which corresponds to the time since the last synchronisation pulse. In the SPC-600, if the arrival time of a photon lies between two different macrotimes the recorded macrotime is rounded up or down in an arbitrary way which means that it is not possible to accurately measure the arrival times of photons in FIFO mode [154], [155], [153]. This makes it unsuitable for use in QKD systems where the timing information of the arrival of the photon is important since the start of the measurement is all important. In modern TCSPC modules like PicoQuant's Hydraharp 400 [156], the role of the time-to-analogue (TAC) and the analogue-to-digital (ADC) converters have been largely replaced by a time to digital converter (TDC) [157]. When operated in "Time Tag Time Resolved" (TTTR) mode it allows for the continuous collection of data. The HydraHarp is operated in "start stop" mode unlike conventional TCSPC due to independent operation of the two time digitisers and a programmable divider in front of the sync input.

2.12.2 Time interval analysis

The measurement of accurate time intervals has many applications which include navigation systems, radar ranging, and telecommunication systems. The time interval T is measured between the leading edges of two electrical pulses which are applied to the start and stop of a time-to digital converter. In its most basic mode of operation, measuring the time interval involves using a counter which is controlled by a reference clock (frequency f). Clock pulses are accumulated for the duration of the gate, shown in Figure 2.54. In a one shot measurement (period from one START pulse to one STOP pulse) the resolution is determined by the clock frequency. In most devices this limits the resolution to about 1 ns resolution. To achieve picosecond resolution averaging techniques can be used in which a series of measurements are performed and then averaged. This method is based on the assumption that contributions to timing jitter are random and when averaged tend to zero [158].

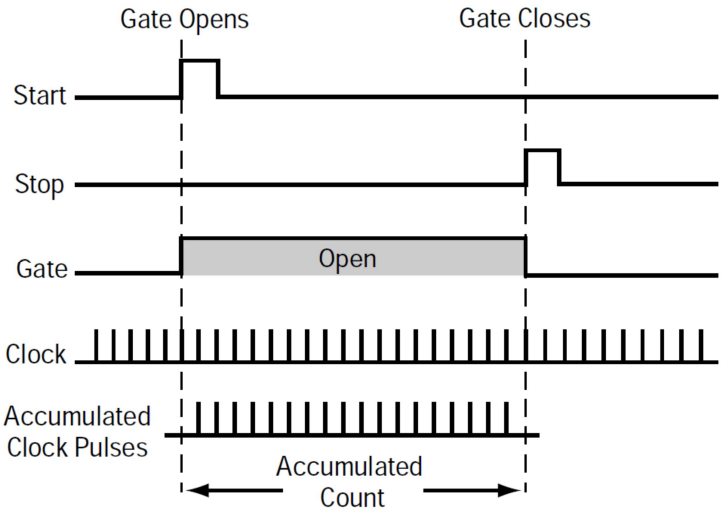

Figure 2.54. In a time interval measurement, clock pulses are accumulated for the duration the main gate is open. The gate is opened by one event, start and closed by the other stop [159].

TIAs are usually grouped into one of two categories either START-to-STOP time interval analysers or time stamp analysers. START-to-STOP TIAs are devices which only measure the timing from a START event relative to a previous STOP event. Time stamp analysers (like the Guidetech GT658PCI [160]) are devices where all event timings are measured relative to a unique reference [161]. Quite often the signals that are to be measured are asynchronous to the clock and therefore there are zones of time which are shorter than the clock which cannot be counted. This fractional or residual times lie at the starting or ending edge of a measurement interval (Figure 2.55). Most TIAs make use of at least one high resolution time interval measurement circuit. A reference clock counter is used to count the number of precise clock cycles within the time interval of the measurement and an interpolator to measure any residual time which is less than one cycle of the reference clock. Circuits to implement this approach include delay chain, vernier delay line, vernier oscillator and time-to-voltage techniques. With delay chain techniques the time interval is quantised with a quantisation step which is given by the unit gate delay which limits the resolution. Vernier delay line techniques use the difference in delay between two delay elements to quantise the time and offer better timing resolution but at the expense of linearity and limited measurement range. Vernier oscillator methods make use of the difference between two oscillator clock periods to quantise the time interval. Time-to-voltage converters charge or discharge during the time interval of the measurement. The

voltage at the end of the time interval indicates the time interval or it's residual relative to the clock reference. The general architect of a TIA device is shown in Figure 2.55.

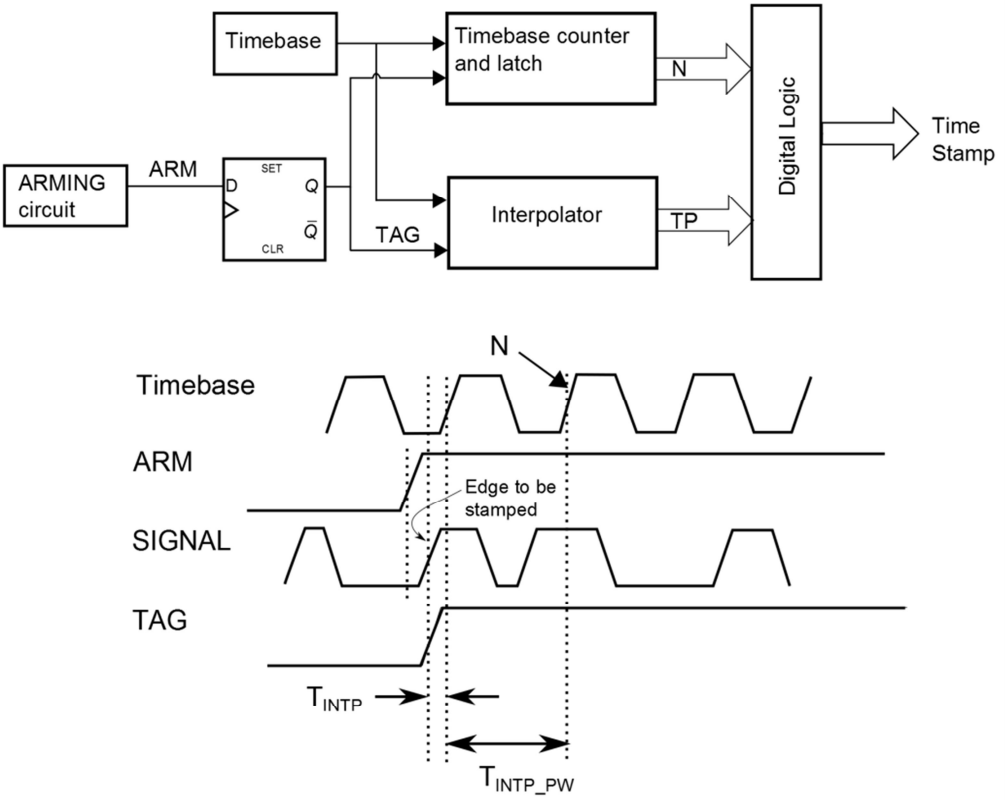

Figure 2.55. The time interval analyser uses an accurate and stable time base and a counter to measure the event timing with a resolution of one time base. An interpolator then measures the event timing to the closest subsequent edge of the time base. The digital logic circuit is used to combine signal N from the counter with the signal from the interpolator to produce the time stamp [161]. T_{INTP} *is the time base residual time. This is the time between the selected input edge and the following time base rising edge and determines the edge timing relative to the time base.* T_{TB} *is the time base average period,* T_{INTP_PW} *is the interpolator pulse width. For above* $T_{INTP\_PW} = T_{TB} + T_{INTP}$.

2.13 Conclusions

This chapter has given a brief overview of some topics in classical cryptography and the development towards quantum key distribution. The enabling technologies for QKD which developed in tandem with the field were also described namely the generation and detection of single-photons.

References

[1] S. Singh, "*The code book: the evolution of secrecy from Mary, Queen of Scots, to quantum cryptography"* 1999: Doubleday.

[2] L.D. Smith, "*Cryptography: the science of secret writing"* 1955: Dover Pubns.

[3] C. Shannon, "*A mathematical theory of communication"*. Bell Labs System Technical Journal 1948. **27**(1): p. 379-423, 623-656.

[4] H. Delfs and H. Knebl, "*Introduction to cryptography: principles and applications"* 2007: Springer-Verlag New York Inc.

[5] W. Diffie and M. Hellman, "*New directions in cryptography"*. IEEE Transactions on information Theory, 1976. **22**(6): p. 644-654.

[6] R. Rivest, A. Shamir, and L. Adleman, "*A method for obtaining digital signatures and public-key cryptosystems"*. Communications of the ACM, 1978. **21**(2): p. 120-126.

[7] T. Kleinjung, K. Aoki, J. Franke, A. Lenstra, E. Thomé, J. Bos, P. Gaudry, A. Kruppa, P. Montgomery, D. Osvik, H. te Riele, A. Timofeev, and P. Zimmermann, "*Factorization of a 768-Bit RSA Modulus"*, in *Advances in Cryptology–CRYPTO 2010*, T. Rabin, Editor 2010, Springer Berlin / Heidelberg. p. 333-350.

[8] P.W. Shor. "*Algorithms for quantum computation: discrete logarithms and factoring"*. in *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*. 1994.

[9] L.M.K. Vandersypen, M. Steffen, G. Breyta, C.S. Yannoni, M.H. Sherwood, and I.L. Chuang, "*Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance"*. Nature, 2001. **414**(6866): p. 883-887.

[10] S. Wiesner, "*Conjugate coding"*. ACM Sigact News, 1983. **15**(1): p. 78-88.

[11] G. Brassard. "*Brief history of quantum cryptography: A personal perspective"*. in *Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information Theoretic Security*. 2005. Awaji Island, Japan: IEEE.

[12] C.H. Bennett and G. Brassard. "*Quantum cryptography: Public key distribution and coin tossing"*. in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. 1984. Bangalore, India.

[13] W. Wootters and W. Zurek, "*A single quantum cannot be cloned"*. Nature, 1982. **299**: p. 802-803.

[14] W. Heisenberg, "*Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik"*. Zeitschrift für Physik A Hadrons and Nuclei, 1927. **43**(3): p. 172-198.

[15] G. Van Assche, "*Quantum cryptography and secret-key distillation"* 2006: Cambridge University Press.

[16] C.H. Bennett, "*Quantum cryptography using any two nonorthogonal states"*. Physical Review Letters, 1992. **68**(21): p. 3121-3124.

[17] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "*Quantum cryptography"*. Reviews of Modern Physics, 2002. **74**(1): p. 145-195.

[18] P. Townsend, J. Rarity, and P. Tapster, "*Single photon interference in 10 km long optical fibre interferometer"*. Electronics Letters, 1993. **29**(7): p. 634-635.

[19] I.D. Ivanovic, "*How to differentiate between non-orthogonal states"*. Physics Letters A, 1987. **123**(6): p. 257-259.

[20] B. Huttner, A. Muller, J.D. Gautier, H. Zbinden, and N. Gisin, "*Unambiguous quantum measurement of nonorthogonal states"*. Physical Review A, 1996. **54**(5): p. 3783-3789.

[21] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "*Fast and simple one-way quantum key distribution"*. Applied Physics Letters, 2005. **87**(19): p. 194108-194108-3.

[22] K. Inoue, E. Waks, and Y. Yamamoto, "*Differential Phase Shift Quantum Key Distribution"*. Physical Review Letters, 2002. **89**(3): p. 037902.

[23] F. Grosshans and P. Grangier, "*Continuous Variable Quantum Cryptography Using Coherent States"*. Physical Review Letters, 2002. **88**(5): p. 057902.

[24] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, "*Field test of a continuous-variable quantum key distribution prototype"*. New Journal of Physics, 2009. **11**(4): p. 045023.

[25] A. Einstein, B. Podolsky, and N. Rosen, "*Can quantum-mechanical description of physical reality be considered complete?"*. Physical Review, 1935. **47**(10): p. 777-780.

[26] J. Bell, "*On the Einstein Podolsky Rosen paradox"*. Physics, 1964. **1**: p. 195-200.

[27] A. Aspect, J. Dalibard, and G. Roger, "*Experimental Test of Bell's Inequalities Using Time- Varying Analyzers"*. Physical Review Letters, 1982. **49**(25): p. 1804-1807.

[28] A. Ekert, "*Quantum cryptography based on Bell's theorem"*. Physical Review Letters, 1991. **67**(6): p. 661-663.

[29] D. Bouwmeester, A.K. Ekert, and A. Zeilinger, "*The physics of quantum information"*. Vol. 38. 2001: Springer.

[30] H. Bechmann-Pasquinucci and W. Tittel, "*Quantum cryptography using larger alphabets"*. Physical Review A, 2000. **61**(6): p. 062308.

[31] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "*"Plug and play" systems for quantum cryptography"*. Applied Physics Letters, 1997. **70**: p. 793.

[32] S. Barnett, "*Quantum information"* 2009: Oxford University Press, USA.

[33] G. Brassard and L. Salvail. "*Secret-key reconciliation by public discussion"*. in *Advances in cryptography- Eurocrypt '93, Lecture Notes in Computer Science*. 1994. Springer.

[34] C. Kollmitzer and M. Pivk, "*Applied quantum cryptography"*. Vol. 797. 2010: Springer Verlag.

[35] N. Lütkenhaus, "*Estimates for practical quantum cryptography"*. Physical Review A, 1999. **59**(5): p. 3301-3319.

[36] C.H. Bennett, G. Brassard, and J.-M. Robert, "*Privacy Amplification by Public Discussion"*. SIAM Journal on Computing, 1988. **17**(2): p. 210-229.

[37] L. Norbert and J. Mika, "*Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack"*. New Journal of Physics, 2002. **4**(1): p. 44.

[38] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "*Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations"*. Physical Review Letters, 2004. **92**(5): p. 057901.

[39] A. Lupascu, S. Saito, T. Picot, P.C. de Groot, C.J.P.M. Harmans, and J.E. Mooij, "*Quantum non-demolition measurement of a superconducting two-level system"*. Nature Physics, 2007. **3**(2): p. 119-125.

[40] V. Makarov, "*Controlling passively quenched single photon detectors by bright light"*. New Journal of Physics, 2009. **11**: p. 065003.

[41] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "*Hacking commercial quantum cryptography systems by tailored bright illumination"*. Nature Photonics, 2010. **4**(10): p. 686-689.

[42] Z. Yuan, J. Dynes, and A. Shields, "*Avoiding the blinding attack in QKD"*. Nature Photonics, 2010. **4**(12): p. 800-801.

[43] Y. Zhao, C.H.F. Fung, B. Qi, C. Chen, and H.K. Lo, "*Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems*". Physical Review A, 2008. **78**(4): p. 042333.

[44] D. Gottesman, H.K. Lo, N. Lutkenhaus, and J. Preskill. "*Security of quantum key distribution with imperfect devices*". in *Quantum Information Computing*. 2004. IEEE.

[45] N. Lutkenhaus, "*Security against individual attacks for realistic quantum key distribution*". Physical Review A, 2000. **61**(052304): p. 1-10.

[46] H.-K. Lo, X. Ma, and K. Chen, "*Decoy state quantum key distribution*". Physical Review Letters, 2005. **94**(2): p. 230504.

[47] C. Gobby, Z. Yuan, and A. Shields, "*Quantum key distribution over 122 km of standard telecom fiber*". Applied Physics Letters, 2004. **84**: p. 3762.

[48] H.-K. Lo, X. Ma, and K. Chen, "*Decoy State Quantum Key Distribution*". Physical Review Letters, 2005. **94**(23): p. 230504.

[49] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "*Experimental quantum cryptography*". Journal of Cryptology, 1992. **5**(1): p. 3-28.

[50] J. Breguet, A. Muller, and N. Gisin, "*Quantum cryptography with polarized photons in optical fibres*". Journal of Modern Optics, 1994. **41**(12): p. 2405-2412.

[51] P. Townsend, "*Secure key distribution system based on quantum cryptography*". Electronics Letters, 1994. **30**(10): p. 809-811.

[52] B. Jacobs and J. Franson, "*Quantum cryptography in free space*". Optics Letters, 1996. **21**(22): p. 1854-1856.

[53] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "*Trojan-horse attacks on quantum-key-distribution systems*". Physical Review A, 2004. **73**: p. 022320.

[54] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, "*Single Photon Quantum Cryptography*". Physical Review Letters, 2002. **89**(18): p. 187901.

[55] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G.S. Solomon, and Y. Yamamoto, "*Secure communication: Quantum cryptography with a photon turnstile*". Nature, 2002. **420**(6917): p. 762-762.

[56] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "*Experimental Quantum Key Distribution with Decoy States*". Physical Review Letters, 2006. **96**(7): p. 070502.

[57] A. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, "*Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate"*. Optics Express, 2008. **16**: p. 18790.

[58] W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden, and N. Gisin, "*Experimental demonstration of quantum correlations over more than 10 km"*. Physical Review A, 1998. **57**(5): p. 3229-3232.

[59] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "*Quantum Cryptography with Entangled Photons"*. Physical Review Letters, 2000. **84**(20): p. 4729.

[60] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "*Entanglement-based quantum communication over 144 km"*. Nature Physics, 2007. **3**(7): p. 481-486.

[61] K.J. Gordon, V. Fernandez, P.D. Townsend, and G.S. Buller, "*A short wavelength gigahertz clocked fiber-optic quantum key distribution system"*. IEEE Journal of Quantum Electronics, 2004. **40**(7): p. 900-908.

[62] H. Takesue, S. Nam, Q. Zhang, R. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "*Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors"*. Nature Photonics, 2007. **1**(6): p. 343-348.

[63] Z.L. Yuan, A.R. Dixon, J.F. Dynes, A.W. Sharpe, and A.J. Shields, "*Gigahertz quantum key distribution with InGaAs avalanche photodiodes"*. Applied Physics Letters, 2008. **92**(20): p. 201104-3.

[64] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "*Current status of the DARPA quantum network"*. Arxiv preprint quant-ph/0503058, 2005.

[65] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, and J. Dynes, "*The SECOQC quantum key distribution network in Vienna"*. New Journal of Physics, 2009. **11**: p. 075001.

[66] M. Fox, "*Quantum optics: an introduction"* 2006: Oxford University Press.

[67] P. Townsend, "*Quantum cryptography on optical fiber networks"*. Optical Fiber Technology, 1998. **4**(4): p. 345-370.

[68] T. Debuisschert and W. Boucher, "*Time coding protocols for quantum key distribution"*. Physical Review A, 2004. **70**: p. 042306.

[69] S. Felix, N. Gisin, A. Stefanov, and H. Zbinden, "*Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses"*. Journal of Modern Optics, 2001. **48**(13): p. 2009-2021.

[70] A.P. Alivisatos, "*Semiconductor clusters, nanocrystals, and quantum dots"*. Science, 1996. **271**(5251): p. 933.

[71] C. Santori, M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto, "*Triggered single photons from a quantum dot"*. Physical Review Letters, 2001. **86**(8): p. 1502-1505.

[72] C. Santori, D. Fattal, J. Vuckovic, G. Solomon, and Y. Yamamoto, "*Single-photon generation with InAs quantum dots"*. New Journal of Physics, 2004. **6**(1): p. 89.

[73] Z. Jacob, I.I. Smolyaninov, and E.E. Narimanov, "*Broadband Purcell effect: Radiative decay engineering with metamaterials"*. Applied Physics Letters, 2012. **100**(18): p. 181105-181105-4.

[74] M. Benyoucef, S. Ulrich, P. Michler, J. Wiersig, F. Jahnke, and A. Forchel, "*Correlated photon pairs from single (In, Ga) As/ GaAs quantum dots in pillar microcavities"*. Journal of Applied Physics, 2005. **97**: p. 023101.

[75] C. Santori, G. Solomon, M. Pelton, and Y. Yamamoto, "*Time-resolved spectroscopy of multiexcitonic decay in an InAs quantum dot"*. Physical Review Series B, 2002. **65**(7): p. 73310-73310.

[76] D. Leonard, M. Krishnamurthy, C. Reaves, S. Denbaars, and P. Petroff, "*Direct formation of quantum sized dots from uniform coherent islands of InGaAs on GaAs surfaces"*. Applied Physics Letters, 1993. **63**(23): p. 3203-3205.

[77] C. Priester and M. Lannoo, "*Origin of Self-Assembled Quantum Dots in Highly Mismatched Heteroepitaxy"*. Physical Review Letters, 1995. **75**(1): p. 93.

[78] S. Kohmoto, H. Nakamura, T. Ishikawa, and K. Asakawa, "*Site-controlled self-organization of individual InAs quantum dots by scanning tunneling probe-assisted nanolithography"*. Applied Physics Letters, 1999. **75**(22): p. 3488-3490.

[79] H. Soda, "*GaInAsP/InP surface emitting injection lasers"*. Japanese Journal of Applied Physics, 1979. **18**(12): p. 2329-2330.

[80] Y. Motegi, H. Soda, and K. Iga, "*Surface-emitting GaInAsP/InP injection laser with short cavity length"*. Electronics Letters, 1982. **18**(11): p. 461-463.

[81] I. Melngailis, "*Longitudinal injection plasma laser of InSb"*. Applied Physics Letters, 1965. **6**: p. 59.

[82] Z. Alferov, V. Andreyev, S. Gurevich, R. Kazarinov, V. Larionov, M. Mizerov, and E. Portnoy, "*Semiconductor lasers with the light output through the diffraction grating on the surface of the waveguide layer"*. Quantum Electronics, IEEE Journal of, 1975. **11**(7): p. 449-451.

[83] S. Blokhin, J. Lott, A. Mutig, G. Fiol, N. Ledentsov, M. Maximov, A. Nadtochiy, V. Shchukin, and D. Bimberg, "*Oxide-confined 850 nm VCSELs operating at bit rates up to 40 Gbit/s"*. Electronics Letters, 2009. **45**(10): p. 501-503.

[84] C. Marand and P. Townsend, "*Quantum key distribution over distances as long as 30 km"*. Optics Letters, 1995. **20**(16): p. 1695.

[85] P. Hiskett, D. Rosenberg, C. Peterson, R. Hughes, S. Nam, A. Lita, A. Miller, and J. Nordholt, "*Long-distance quantum key distribution in optical fibre"*. New Journal of Physics, 2006. **8**: p. 193.

[86] V. Fernandez, R.J. Collins, K.J. Gordon, P.D. Townsend, and G.S. Buller, "*Passive optical network approach to gigahertz-clocked multiuser quantum key distribution"*. IEEE Journal of Quantum Electronics, 2007. **43**(2): p. 130-138.

[87] A.L. Migdall, D. Branning, and S. Castelletto, "*Tailoring single-photon and multiphoton probabilities of a single-photon on-demand source"*. Physical Review A, 2002. **66**(5): p. 053805.

[88] S. Fasel, O. Alibart, S. Tanzilli, P. Baldi, A. Beveratos, N. Gisin, and H. Zbinden, "*High-quality asynchronous heralded single-photon source at telecom wavelength"*. New Journal of Physics, 2004. **6**: p. 163.

[89] E.A. Goldschmidt, M.D. Eisaman, J. Fan, S.V. Polyakov, and A. Migdall, "*Spectrally bright and broad fiber-based heralded single-photon source"*. Physical Review A, 2008. **78**(1): p. 013844.

[90] A.R. McMillan, J. Fulconis, M. Halder, C. Xiong, J.G. Rarity, and W.J. Wadsworth, "*Narrowband high-fidelity all-fibre source of heralded single photons at 1570 nm"*. Optics Express, 2009. **17**(8): p. 6156-6165.

[91] A. Soujaeff, S. Takeuchi, K. Sasaki, T. Hasegawa, and M. Matsui, "*Heralded single photon source at 1550 nm from pulsed parametric down conversion"*. Journal of Modern Optics, 2007. **54**(2-3): p. 467-471.

[92] A. Hayat, P. Ginzburg, and M. Orenstein, "*Observation of two-photon emission from semiconductors"*. Nature Photonics, 2008. **2**(4): p. 238-241.

[93] R. Brouri, A. Beveratos, J. Poizat, and P. Grangier, "*Photon antibunching in the fluorescence of individual color centers in diamond"*. Optics Letters, 2000. **25**(17): p. 1294-1296.

[94] C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter, "*Stable solid-state source of single photons"*. Physical Review Letters, 2000. **85**(2): p. 290-293.

[95] A. Gruber, A. Dräbenstedt, C. Tietz, L. Fleury, J. Wrachtrup, and C. Borczyskowski, "*Scanning confocal optical microscopy and magnetic resonance on single defect centers"*. Science, 1997. **276**(5321): p. 2012.

[96] M.D. Eisaman, J. Fan, A. Migdall, and S.V. Polyakov, "*Invited Review Article: Single-photon sources and detectors"*. Review of Scientific Instruments, 2011. **82**(7): p. 071101.

[97] R.H. Brown and R. Twiss, "*Correlation between photons in two coherent beams of light"*. Nature, 1956. **177**(4497): p. 27-29.

[98] R. Loudon, "*Non-classical effects in the statistical properties of light"*. Reports on Progress in Physics, 1980. **43**: p. 913.

[99] P.R. Berman and E. Arimondo, "*Advances in atomic, molecular, and optical physics"*. Vol. 54. 2006: Academic Press.

[100] N. Mizuochi, T. Makino, H. Kato, D. Takeuchi, M. Ogura, H. Okushi, M. Nothaft, P. Neumann, A. Gali, and F. Jelezko, "*Electrically driven single-photon source at room temperature in diamond"*. Nature Photonics, 2012. **6**(5): p. 299-303.

[101] K. Resch, M. Lindenthal, B. Blauensteiner, H. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, and R. Ursin, "*Distributing entanglement and single photons through an intra-city, free-space quantum channel"*. Optics Express, 2005. **13**(1): p. 202-209.

[102] R. Ramaswami, "*Optical fiber communication: From transmission to networking"*. Communications Magazine, IEEE, 2002. **40**(5): p. 138-147.

[103] *"Corning SMF-28 Optical Fiber", Corning,2002, http://www.corning.com/WorkArea/showcontent.aspx?id=41261, date accessed:23/5/2012*

[104] J. Wilson and J.F.B. Hawkes, "*Optoelectronics-an introduction"*. 1989.

[105] *"Fiber Types in Gigabit Optical Communications", Cisco Systems,2008, http://www.cisco.com/en/US/prod/collateral/modules/ps5455/white_paper_c11-463661.pdf, date accessed:2/4/2012*

[106] G. Keiser, "*Optical fiber communications"* 2000: McGraw-Hill.

[107] A. Kumar and A.K. Ghatak, "*Polarization of light with applications in optical fibers"* 2011: SPIE Press.

[108] D. Subacius, A. Zavriyev, and A. Trifonov, "*Backscattering limitation for fiber-optic quantum key distribution systems"*. Applied Physics Letters, 2005. **86**(1): p. 011103-3.

[109] I.P. Choi, R.J. Young, and P.D. Townsend, "*Quantum information to the home"*. New Journal of Physics, 2011. **13**(6): p. 063039.

[110] I. Choi, R.J. Young, and P.D. Townsend, "*Quantum key distribution on a 10Gb/s WDM-PON"*. Optical Express, 2010. **18**(9): p. 9600-9612.

[111] G.S. Buller and R.J. Collins, "*Single-photon generation and detection"*. Measurement Science and Technology, 2010. **21**: p. 012002.

[112] C. Adams, I. Hughes, C. Webb, and J. Jones, "*Handbook of Laser Technology and Applications"*, 2004, Edited by: Webb, CE and Jones, JDC. London: Institute of Physics.

[113] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, "*Avalanche photodiodes and quenching circuits for single-photon detection"*. Applied Optics, 1996. **35**(12): p. 1956-1976.

[114] S. Cova, A. Lacaita, M. Ghioni, G. Ripamonti, and T. Louis, "*20 ps timing resolution with single photon avalanche diodes"*. Review of Scientific Instruments, 1989. **60**(6): p. 1104-1110.

[115] R.J. McIntyre, "*Multiplication noise in uniform avalanche diodes"*. IEEE Transactions on Electron Devices, 1966. **13**(1): p. 164-168.

[116] J.C. Patrick, J.C. Robert, A.H. Philip, G.-M. María-José, J.K. Nils, M. Aongus, G.T. Michael, A.O.C. John, M.N. Chandra, M. Shigehito, S. Masahide, W. Zhen, F. Mikio, R. Ivan, G. Massimo, G. Angelo, H.H. Robert, D.T. Paul, and S.B. Gerald, "*Analysis of detector performance in a gigahertz clock rate quantum key distribution system"*. New journal of physics, 2011. **13**(7): p. 075008.

[117] S. Tudisco, F. Musumeci, L. Lanzano, A. Scordino, S. Privitera, A. Campisi, L. Cosentino, G. Condorelli, P. Finocchiaro, and G. Fallica, "*A New Generation of SPAD—Single-Photon Avalanche Diodes"*. Sensors Journal, IEEE, 2008. **8**(7): p. 1324-1329.

[118] A. Lacaita, M. Ghioni, and S. Cova, "*Double epitaxy improves single-photon avalanche diode performance"*. Electronics Letters, 1989. **25**(13): p. 841-843.

[119] H. Dautet, P. Deschamps, B. Dion, A. MacGregor, D. MacSween, R. McIntyre, C. Trottier, and P. Webb, "*Photon counting techniques with silicon avalanche photodiodes"*. Applied Optics, 1993. **32**(21): p. 3894-3900.

[120] R.G.W. Brown, K.D. Ridley, and J.G. Rarity, "*Characterization of silicon avalanche photodiodes for photon correlation measurements. 1: Passive quenching"*. Applied Optics, 1986. **25**(22): p. 4122-4126.

[121] M. Ghioni and G. Ripamonti, "*Improving the performance of commercially available Geiger mode avalanche photodiodes"*. Review of Scientific Instruments, 1991. **62**(1): p. 163-167.

[122] J.G. Rarity, T.E. Wall, K.D. Ridley, P.C.M. Owens, and P.R. Tapster, "*Single-Photon Counting for the 1300-1600-nm Range by Use of Peltier-Cooled and Passively Quenched InGaAs Avalanche Photodiodes"*. Appied Optics, 2000. **39**(36): p. 6746-6753.

[123] Z.L. Yuan, A.W. Sharpe, J.F. Dynes, A.R. Dixon, and A.J. Shields, "*Multi-gigahertz operation of photon counting InGaAs avalanche photodiodes"*. Applied Physics Letters, 2010. **96**(7): p. 071101-3.

[124] G. Buller, R. Warburton, S. Pellegrini, J. Ng, J. David, L. Tan, A. Krysa, and S. Cova, "*Single-photon avalanche diode detectors for quantum key distribution"*. Optoelectronics, IET, 2007. **1**(6): p. 249-254.

[125] A. Lacaita, P.A. Francese, F. Zappa, and S. Cova, "*Single-photon detection beyond 1 μm: performance of commercially available germanium photodiodes"*. Applied Optics, 1994. **33**(30): p. 6902-6918.

[126] A. Spinelli and A.L. Lacaita, "*Physics and numerical simulation of single photon avalanche diodes"*. IEEE Transactions on Electron Devices, 1997. **44**(11): p. 1931-1943.

[127] M.S. Unlu and S. Strite, "*Resonant cavity enhanced photonic devices"*. Journal of Applied Physics, 1995. **78**(2): p. 607-639.

[128] M. Ghioni, G. Armellini, P. Maccagnani, I. Rech, M.K. Emsley, and M.S. Ünlü, "*Resonant-cavity-enhanced single photon avalanche diodes on double silicon-on-insulator substrates"*. Journal of Modern Optics, 2009. **56**(2-3): p. 309-316.

[129] K.D. Irwin and G.C. Hilton, "*Transition-Edge Sensors"*, 2005, Springer Berlin / Heidelberg. p. 81-97.

[130] B. Cabrera, R.M. Clarke, P. Colling, A.J. Miller, S. Nam, and R.W. Romani, "*Detection of single infrared, optical, and ultraviolet photons using*

superconducting transition edge sensors". Applied Physics Letters, 1998. **73**(6): p. 735-737.

[131] D. Rosenberg, A.E. Lita, A.J. Miller, and S.W. Nam, "*Noise-free high-efficiency photon-number-resolving detectors".* Physical Review A, 2005. **71**(6): p. 061803.

[132] W.S. Holland, W. Duncan, B.D. Kelly, K.D. Irwin, A.J. Walton, P.A.R. Ade, and E.I. Robson. "*SCUBA-2: a large-format submillimeter camera on the James Clerk Maxwell Telescope".* 2003. Waikoloa, HI, USA: SPIE.

[133] J. Ray, S.H. Wayne, S.G. Jane, R.F.D. William, W.M. Geoffrey, W.H. Lee, and G.F. Giovanni, "*Dust in the 55 Cancri Planetary System".* The Astrophysical Journal, 2000. **536**(1): p. 425.

[134] A. Verevkin, A. Pearlman, W. Slysz, J. Zhang, M. Currier, A. Korneev, G. Chulkova, O. Okunev, P. Kouminov, and K. Smirnov, "*Ultrafast superconducting single-photon detectors for near-infrared-wavelength quantum communications".* Journal of Modern Optics, 2004. **51**(9-10): p. 1447-1458.

[135] L. Cooper, "*Bound electron pairs in a degenerate Fermi gas".* Physical Review, 1956. **104**(4): p. 1189-1190.

[136] G. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski, "*Picosecond superconducting single-photon optical detector".* Applied Physics Letters, 2001. **79**: p. 705.

[137] G. Gol'Tsman, A. Semenov, Y.P. Gousev, M. Zorin, I. Godidze, E. Gershenzon, P. Lang, W. Knott, and K. Renk, "*Sensitive picosecond NbN detector for radiation from millimetre wavelengths to visible light".* Superconductor Science and Technology, 1991. **4**: p. 453.

[138] R.H. Hadfield, J.L. Habif, J. Schlafer, R.E. Schwall, and S.W. Nam, "*Quantum key distribution at 1550 nm with twin superconducting single-photon detectors".* Applied Physics Letters, 2006. **89**: p. 241129.

[139] K. Hamamatsu Photonics and E. Committee, "*Photomultiplier Tubes-Basics and Applications".* Hamamatsu Photonics KK, 2006: p. 240-242.

[140] *"NIR-PMT Module", Hamamatsu,http://209.73.52.252/assets/pdf/parts_H /H10330.pdf, date accessed:16/6/2012*

[141] A. Shields, M. O'sullivan, I. Farrer, D. Ritchie, R. Hogg, M. Leadbeater, C. Norman, and M. Pepper, "*Detection of single photons using a field-effect*

transistor gated by a layer of quantum dots". Applied Physics Letters, 2000. **76**: p. 3673.

[142] B. Kardynal, A. Shields, N. Beattie, I. Farrer, K. Cooper, and D. Ritchie, "*Low-noise photon counting with a radio-frequency quantum-dot field-effect transistor".* Applied Physics Letters, 2004. **84**: p. 419.

[143] M.A. Rowe, E.J. Gansen, M. Greene, R.H. Hadfield, T.E. Harvey, M.Y. Su, S.W. Nam, R.P. Mirin, and D. Rosenberg, "*Single-photon detection using a quantum dot optically gated field-effect transistor with high internal quantum efficiency".* Applied Physics Letters, 2006. **89**(25): p. 253505-3.

[144] B.E. Kardynal, A.J. Shields, M.P. O'Sullivan, N.S. Beattie, I. Farrer, D.A. Ritchie, and K. Cooper, "*Detection of single photons using a field effect transistor with a layer of quantum dots".* Measurement Science and Technology, 2002. **13**(11): p. 1721.

[145] A. Divochiy, F. Marsili, D. Bitauld, A. Gaggero, R. Leoni, F. Mattioli, A. Korneev, V. Seleznev, N. Kaurova, O. Minaeva, G. Gol'tsman, K.G. Lagoudakis, M. Benkhaoul, F. Levy, and A. Fiore, "*Superconducting nanowire photon-number-resolving detector at telecommunication wavelengths".* Nature Photonics, 2008. **2**(5): p. 302-306.

[146] B.E. Kardynal, Z.L. Yuan, and A.J. Shields, "*An avalanche photodiode-based photon-number-resolving detector".* Nature Photonics, 2008. **2**(7): p. 425-428.

[147] Z. Lijian, N. Leonardo, S.L. Jeff, and A.W. Ian, "*A characterization of the single-photon sensitivity of an electron multiplying charge-coupled device".* Journal of physics B: atomic, molecular and optical physics, 2009. **42**(11): p. 114011.

[148] *"IXon Ultra 897 Datasheet", Andor Technologies, Northern Ireland,2012, http://www.andor.com/pdfs/specifications/Andor_iXon_Ultra_897_Specifications.pdf, date accessed:23/5/2012*

[149] L.A. Lugiato, A. Gatti, and E. Brambilla, "*Quantum imaging".* Journal of Optics B: Quantum and Semiclassical Optics, 2002. **4**(3): p. S176.

[150] Y.T. Didenko, W.B. McNamara, and K.S. Suslick, "*Molecular emission from single-bubble sonoluminescence".* Nature, 2000. **407**(6806): p. 877-879.

[151] K. Palo, L. Brand, C. Eggeling, S. Jäger, P. Kask, and K. Gall, "*Fluorescence intensity and lifetime distribution analysis: toward higher accuracy in fluorescence fluctuation spectroscopy".* Biophysical Journal, 2002. **83**(2): p. 605-618.

[152] S. Cova, M. Bertolaccini, and C. Bussolati, "*The measurement of luminescence waveforms by single-photon techniques"*. Physica Status Solidi (a), 1973. **18**(1): p. 11-62.

[153] W. Becker, "*The bh TCSPC handbook"*. Becker & Hickl GmbH, 2008.

[154] W. Becker, "*Advanced time-correlated single photon counting techniques"*. Vol. 81. 2005: Springer Verlag.

[155] W. Becker, A. Bergmann, C. Biskup, L. Kelbauskas, T. Zimmer, N. Klöcker, and K. Benndorf. "*High resolution TCSPC lifetime imaging"*. 2003.

[156] *"HydraHarp 400-multi channel picosecond event time", PicoQuant GmbH, Berlin, Germany,2011, http://www.picoquant.com/datasheets/photon_counting/HydraHarp400.pdf, date accessed:15/6/2012*

[157] M. Wahl, H.J. Rahn, T. Röhlicke, G. Kell, D. Nettels, F. Hillger, B. Schuler, and R. Erdmann, "*Scalable time-correlated photon counting system with multiple independent input channels"*. Review of Scientific Instruments, 2008. **79**: p. 123113.

[158] K. Józef, "*Review of methods for time interval measurements with picosecond resolution"*. Metrologia, 2004. **41**(1): p. 17.

[159] *"Fundamentals of Time Interval Measurements", Hewlett-Packard,1997, http://ilrs.gsfc.nasa.gov/docs/time_interval_measurements.pdf, date accessed:10/5/2012*

[160] *"PC-based time interval analyser GT658", http://www.guidetech.com/gt-658, date accessed:10/5/2012*

[161] S. Tabatabaei, *"High resolution time interpolator"*, Guide Technology, Inc. (Sunnyvale, CA, US), patent number 8064293, 2011

Chapter 3

Quantum dot micropillar cavity for quantum key distribution

3.1 Introduction

The generation of single-photons on demand has many useful applications in quantum communication and quantum information processing. Single-photon sources (SPS) have been used in quantum teleportation systems, in which a quantum state can be transmitted and reconstructed over arbitrary long distances [1]. Single-photons can also be used to build universal quantum gates using only linear optics [2] which is fundamental for quantum information processing. Probably the most widespread use of single-photon sources in quantum information has been in quantum key distribution (QKD) systems. In the infancy of quantum cryptography many QKD systems used a highly attenuated laser beam with an average of 0.1 photons per pulse in order to approximate a single photon source [3]. The problem of using such a classical light source is that the photon number distribution is determined by Poissonian statistics. Laser sources which are attenuated to less than one photon per pulse on average still have a probability of containing more than more photon [4]. Such a case would present a potential eavesdropper with the opportunity to use an intercept-resend attack to gain information about the key. Obviously then a perfect single-photon emitter which exhibits true single-photon characteristics would be beneficial in a quantum key distribution system. To meet this challenge this chapter looks at the characterisation of a quantum dot emitting at a wavelength of 894 nm and its integration into a QKD system implementing the BB84 protocol using polarisation encoding. The benefits of using a SPS over an attenuated laser pulse in a QKD environment are also discussed.

3.2 Semiconductor quantum dots

Semiconductor quantum dots are a particular type of semiconductor structure which confines the motion of an electron in all three dimensions. This confinement to length scales smaller than the de Broglie wavelength $\lambda = h/p$, where h is Plank's constant and p is the momentum, results in an electronic structure with discrete energy levels [5]. The directionality and the emission characteristics of a quantum dot (QD) can be altered if it is placed within a cavity. Dots contained within cavities tend to have higher collection efficiencies than those in bulk semiconductors. Examples include micropillar, disk, and photonic crystal cavities shown in Figure 3.1. Cavity

enhancement in photonic crystal waveguides involves introducing a point defect in a 2D photonic crystal. The photonic bandgap is used for optical confinement in the transverse direction while total internal reflection between the air-slab interface provides confinement in the longitudinal direction.

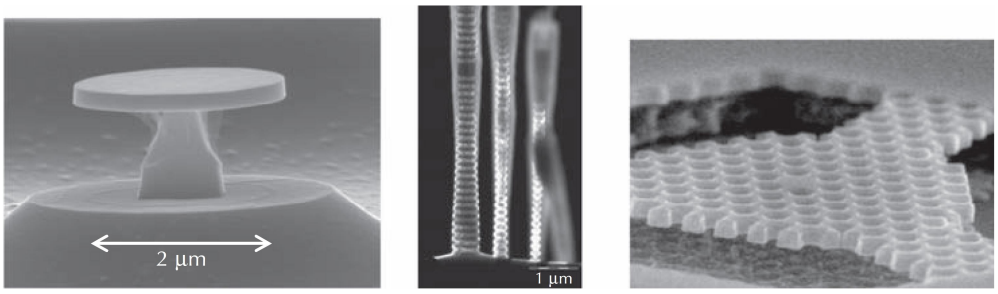

Figure 3.1. Images of different semiconductor cavity geometries, (left) 2 µm diameter GaAs microdisk, (centre) AlGaAs/GaAs micropillar and (right) photonic crystal cavities etched on a 180 nm thick GaAs membrane [6].

Optical confinement in a microdisk cavity is obtained by the high index contrast ratio between the air and the disk and confines the optical mode to the plane of the disk ensuring interaction with the dot. However, these devices tend to suffer from poor collection efficiencies due to the distribution of optical modes around the entire disk.

3.2.1 Excitation and recombination processes in semiconductor quantum dots

The optical spectra of quantum dots can be understood by examining the electronic shell structure, the spin structure and the interactions between electrons and holes. The excitation and relaxation processes are seen in Figure 3.2. An optical excitation pulse creates carriers in the wetting layer or higher quantum dot states. Fast scattering (~1-100 ps) relaxes the carriers into the lower quantum states by carrier-carrier and carrier-phonon interactions. The quantum states are solely populated at low temperatures and low carrier concentrations [7]. The emission energies of the quantum dot can be altered if more than one electron-hole pair is in the quantum dot. If two electron-hole pairs are created (biexciton), the emission of the first pair is at slightly lower energies than the second pair due to Coulomb interactions between the pairs [8]. The quantum dot may be excited by non-resonant methods in which excitation occurs into the wetting layer, and by resonant methods into the s-shell. Non-resonant excitation has the drawback of increasing the timing jitter of the emission process and also defect centres near the quantum dot can capture the carriers. Resonant excitation, into the s-shell has the

benefit of a timing jitter due solely to the radiative lifetime and allows the emission from a single dot to be selected [9].

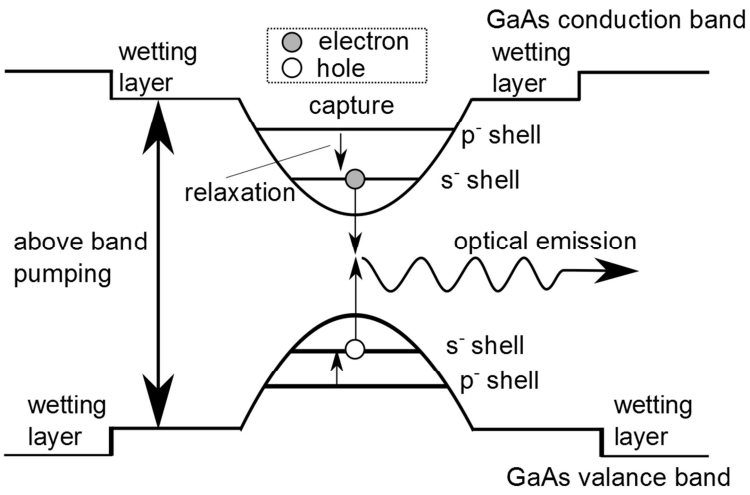

Figure 3.2. Schematic showing carrier capture from a GaAs barrier into a QD and carrier relaxation within the QD. Both the conduction and the valence band have p^- and s^- shells. A thin 2D InAs layer is formed during the growth process and is referred to as the wetting layer [6].

Experimentally it is more challenging as it requires a tuneable laser to exactly match the desired transition and [7] separating the strong pump signal from the weaker emitted signal at the same wavelength is more difficult. Quantum dots can also be electrically excited [10] and offer many simplifications over optical excitation. In many working demonstrations of the device, the quantum dot is located in the intrinsic region of a p-i-n junction (p-type, intrinsic and n-type semiconductor region). The mesa containing the quantum dot can be apertured so that emission from a single dot can be collected. Other single-photon turnstile devices use the Coulomb blockage effect for both electrons and holes, to precisely control the charge transport, one by one, into p-n junction type devices [11].

3.3 Quantum dot micropillar cavities

Employing growth techniques and different material combinations quantum dots have been made to emit at various wavelengths, at 850 nm using InAs/GaAs [12], at 1.3 μm using InAs/GaAs with a capping layer of InGaAs, which acts as a strain relief layer (SRL) [13] and at 1.5 um using InAs/InP [14]. InAs quantum dots with an $In_xGa_{1-x}As$ strain relief layer can be tuned from 1.3 μm to 1.5 μm by changing the indium composition ratio (x value) of the InGaAs SRL. For the experiments conducted in this chapter an InAs quantum dot in a micropillar cavity was used throughout. Optical

confinement in the quantum dot microcavity is obtained through a combination of waveguiding along the pillar and longitudinal confinement by the distributed Bragg reflector (DBR). DBR work by employing multiple layers of alternating refractive index material which are a quarter of a wavelength thick. Fresnel reflection occurs off each boundary and light which is 4 times the optical thickness of the layers undergoes constructive interference and act as a high quality reflector. Light which is emitted from the fundamental mode of a microcavity can be approximated as a Gaussian beam which enables it to be more efficiently coupled into optical fibres than free space quantum dots [15]. The DBR is often composed of mirrors consisting of alternating quarter-wavelength thick layers of GaAs and AlAs, which are separated by a one wavelength-thick spacer layer of GaAs. In this scenario the cavity between the DBR mirrors can support a resonant mode with electric field antinodes at the mirrors and the centre of the cavity [16]. The reflectivity of the bottom DBR can be designed to be significantly higher than that of the top DBR by selecting the number of mirror pairs, so that almost all of the light in the cavity escapes upwards rather than downwards. The reflectivity of m double layers each of quarter-wave thickness is given by

$$R = \left(\frac{n_0 n_2^{2m} - n_3 n_1^{2m}}{n_0 n_2^{2m} + n_3 n_1^{2m}} \right)^2 \qquad \text{Equation (3.1)}$$

where n_1 and n_2 are the refractive indices of the dielectric layer and n_0 and n_3 are the refractive indices of the medium above and below respectively [17]. A typical quantum dot micropillar is shown in Figure 3.3.

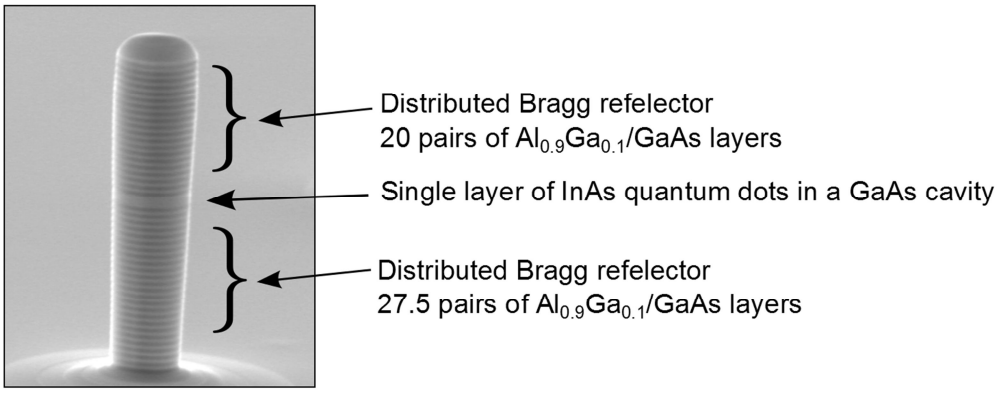

Figure 3.3. A scanning electron microscope (SEM) image of a 2 µm quantum dot pillar grown at the III-V Facility in Sheffield. The quantum dot pillar consists of distributed Bragg reflectors (DBR) of GaAs/AlGaAs layers [18].

In the weak coupling regime the spontaneous emission of the quantum dot in the cavity can be modified compared to how it would emit if outside the cavity by a phenomena which is known as the Purcell effect [19]. The weak coupling regime is defined as when photons are lost from the atom cavity system at a faster rate than the characteristic interaction time between the atom and the cavity [20]. The strong coupling regime occurs when the coupling rate between the emitting atom and the cavity is larger than the photon loss rate which enables a photon to be reabsorbed by the atom before it is lost from the cavity. The Purcell factor is defined as the ratio of the free space radiative lifetime τ_R^{free} to the radiative lifetime of the cavity τ_R^{cavity}. Figure 3.4 photoluminescence trace from a quantum dot micropillar cavity on and off resonance.

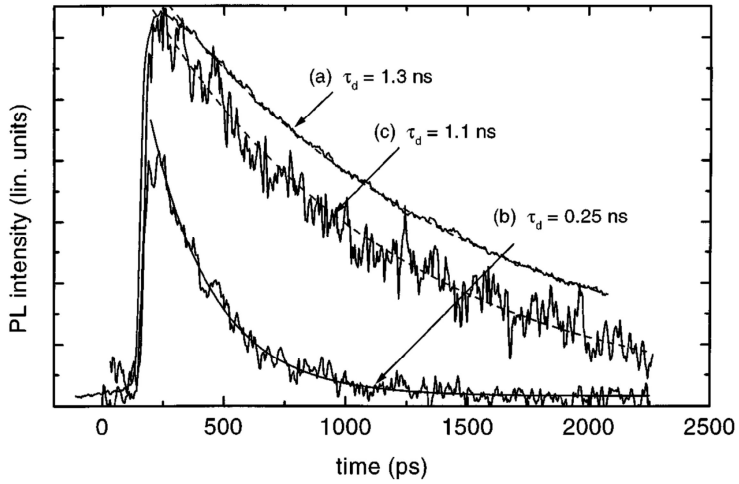

Figure 3.4. Photoluminescence showing a quantum dot micropillar cavity when on resonance and off resonance. The ratio of their decay lifetimes when on and off resonance can be used to calculate the Purcell effect [21].

An increase in the Purcell factor is observed when the emission of the dot is in resonance with the cavity, the emitter is at the antinode of the vacuum field and its dipole is parallel to the vacuum electric field [21]. The modification to the spontaneous emission rate caused by the interaction of the dipole with a single cavity is given by

$$F = \frac{3Q}{4\pi^2 V/\left(\lambda_0/n\right)^3} \times \frac{\Delta\lambda^2{}_c}{4\left(\lambda-\lambda_c\right)^2+\left(\Delta\lambda_c\right)^2} \frac{\left|\vec{u}\left(\vec{r}\right)\cdot\vec{d}\right|^2}{\left|\vec{d}\right|^2} \qquad \text{Equation (3.2)}$$

The first term is the largest spontaneous emission enhancement induced by the cavity mode that can be obtained and depends only on the optical characteristics of the optical

mode, namely the quality factor Q and the effective mode volume V. In Equation (3.2) $\vec{d}$ is the electric dipole moment and $\vec{u}(\vec{r})$ describes the polarisation and the relative amplitude of the electric field at a location $\vec{r}$. This second term considers the spatial overlap and the orientation matching between the transition dipole and the electric field of the cavity mode. The deterministic overlap of the electric field of the dipole and the cavity is challenging during the manufacture stage and many cavity electrodynamics experiments have relied on the random spatial and spectral overlap between the quantum dot and the cavity mode. Badolato *et al.* showed a deterministic way this overlap could be achieved by growing vertical stacks of quantum dots so that their position could be detected by scanning electron microscopy [22]. The third term in the equation represents the spectral detuning between the cavity mode and the emitter, where λ_c is the cavity resonance wavelength and $\Delta\lambda = \lambda_c/Q$ is the cavity linewidth.

3.4 Quantum dot microcavities for QKD

The quantum dot samples were produced at the National Centre of III-V Technologies in Sheffield using the Stranski-Krastanov (SK) growth method also known as self-assembly[23]. SK is a heteroepitaxial growth method based on the deposition of a film on a substrate which has a different lattice constants. The lattice mismatch results in elastic potential energy which must be released. In the case of InAs on GaAs the lattice mismatch is 7%. This energy may be released by the formation of dislocations or the nucleation of three-dimensional islands on top of the flat film (the wetting layer) when the InAs layer thickness reaches a critical value. When the 3D islands are embedded within epitaxial layers of a material which has a larger bandgap, the carriers within the island are confined by the potential barriers of the material that surrounds it forming a quantum dot. The size and density distribution of the quantum dots depend on the growth conditions including substrate temperature and InAs deposition rate [24]. The growth of these dots is referred to as self-assembly as no further processing is required to form the islands. The random nucleation site of the individual quantum dots is an issue when trying to position the dot in a micropillar cavity [25].

The micropillar samples were produced using electron beam lithography (EBL) and inductively coupled plasma etching. The micropillar cavities are spin coated by a polymethyl methacrylate (PMMA) resists which is sensitive to an electron beam. The pillar cross section is written onto this resist using high resolution electron-beam lithography. The resist is then developed so that the exposed regions are removed.

Plasma etching is then used to shape the micropillars out of the semiconductor material [26]. The samples were arranged in a grid-like structure depending on the pillar diameter size. The structure also contained alignment features for easy identification of a particular pillar of interest. The 1 µm diameter quantum dot microcavity structure itself consisted of an InAs quantum dot located in an optical cavity with 16 pairs of distributed Bragg reflector mirrors below the dot layer and six above. The best candidate pillar had been determined from work done previously in the group [27]. The samples were grown specifically to have an emission in the wavelength range 890-905 nm as a comprise to ensure high detection efficiencies (~35% at 894 nm) using thick-junction silicon avalanche photodiodes (SPAD), whose detection efficiency decreases rapidly with increasing wavelength, while at the same time ensuring low loss in standard telecoms fibre (~2.2 dB/km at 894 nm) which decreases in attenuation with increasing wavelength. Figure 3.5 shows the nature of the compromise required between detection efficiency and fibre attenuation.

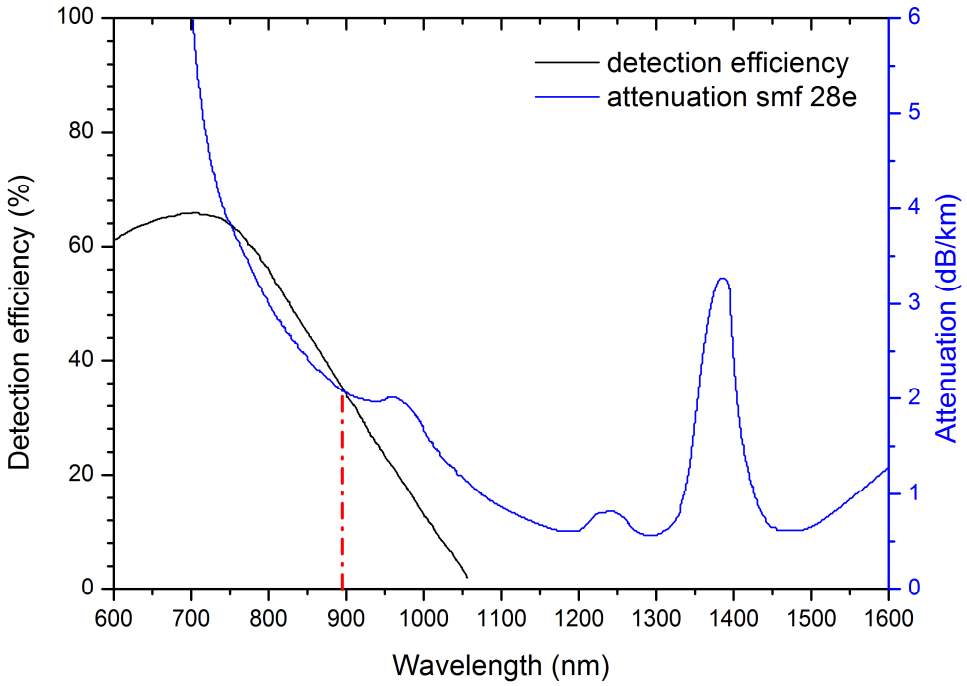

Figure 3.5. Left axis shows the detection efficiency of a commercial Perkin Elmer thick-junction silicon SPAD against wavelength while the right axis shows the attenuation of silica optical fibre against wavelength. At increasing wavelength the fibre loss decreases but this is accompanied by a rapid fall in the detection efficiency of the silicon SPAD [28].

A single transition in a quantum dot was selected by one 55 nm full-width-at-half-maximum (FWHM) bandpass filter centred at 905 nm and two custom made Omega

Optical narrow bandpass filters centred on 894.5 nm with a FWHM of 1.47 nm shown in Figure 3.6.

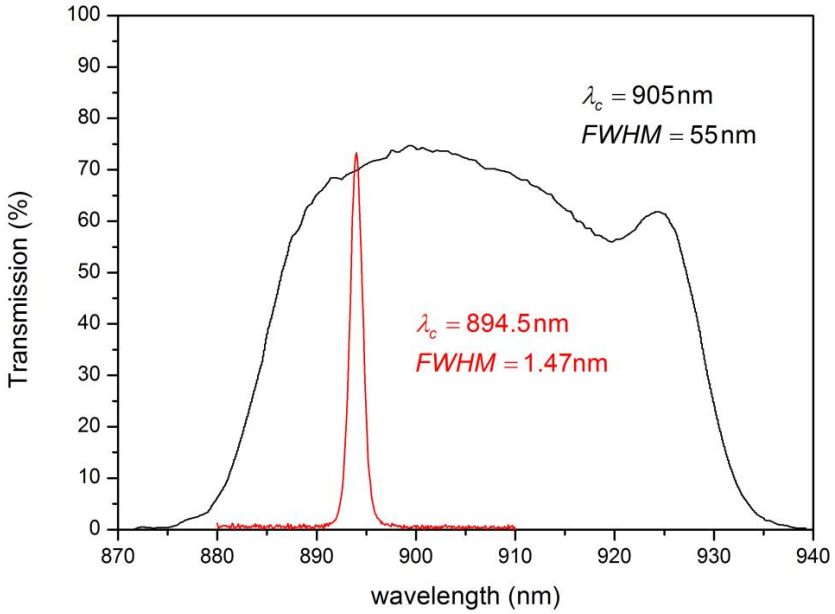

Figure 3.6. The transmission spectra of the narrow (1.47 nm FWHM) and broad (55nm FWHM) filters by Omega Optical used in the quantum dot experiment.

The filters can also reject stray light from the background and from the excitation laser. These filters are based on a Fabry-Pérot etalon whose transmission spectrum shows peaks when the wavelength of the light is in resonance with the etalon. The transmission is given by

$$T(\lambda) = \frac{1}{1 + F\sin^2\left(\frac{\delta(\lambda)}{2}\right)} \qquad \text{Equation (3.3)}$$

where F is the finesse of the cavity and δ is the phase thickness of the film. These filters are designed for operation at normal incidence but as the angle of incidence increases the central wavelength of transmission decreases and the FWHM increases. [29]. The phase thickness of the film is given by $\delta = 2\pi nd\cos/\lambda$, where n is the refractive index, d is the thickness of the film and λ is the wavelength. The optical thickness $nd\cos\theta$ varies with the angle of incidence so that the layer appears optically thinner when tilted. The predicted central wavelength obtained when angle tuning can be given by the following expression

$$\lambda_c = \lambda_0\sqrt{1 - \frac{\sin^2(\theta)}{n_{eff}^{\ 2}}} \qquad \text{Equation (3.4)}$$

where λ_c is the central wavelength, λ_0 is the central wavelength at normal incidence and n_{eff} is the effective index of refraction [30]. Figure 3.7 shows the effect of angle tuning on the central wavelength and the FWHM of the transmission (data obtained previously by the research group).

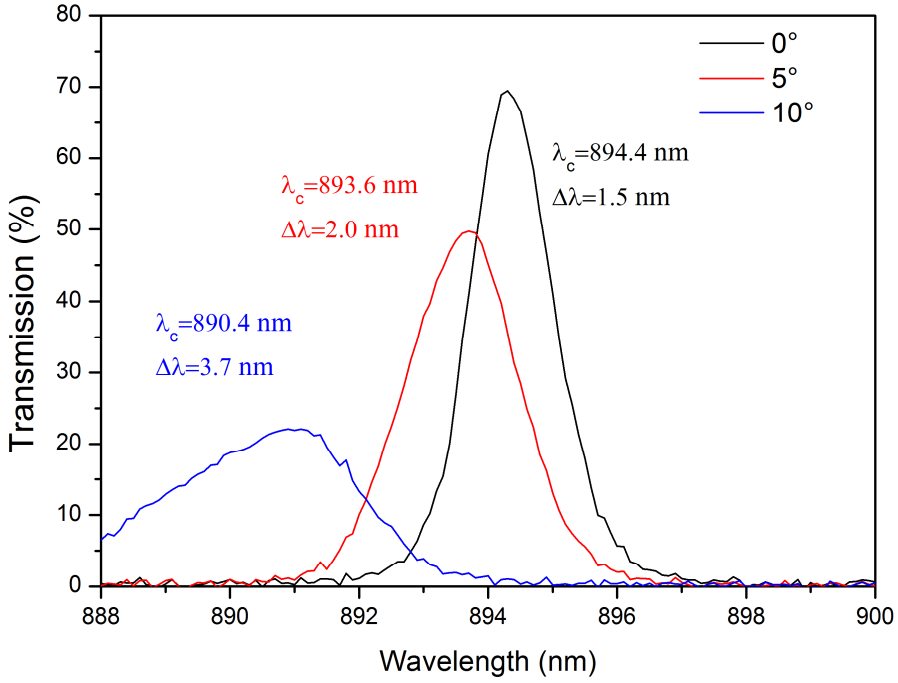

Figure 3.7. The transmission of the narrow bandpass filter (Omega Optical) is shown at three different angles of incidence of the transmitted light. As the angle is increased from zero the central wavelength decreases and the FWHM increases. The central wavelength can be predicted using Equation (3.4). The measured values of the central wavelength are 894.4, 893.6 and 890.4 nm for angles of incidence of 0°, 5° and 10° respectively and agree well with the predicted values of 893.48 and 891.1 nm for angle of 5° and 10° when using $n_{eff} = 2$.

The predicted values for the central wavelength were calculated to be 893.48 nm and 891.1 nm when using $n_{eff} = 2$ which is in close agreement to the measured values of 893.6 nm and 890.4 nm for angles of incidence of 5º and 10º respectively. One of the narrow bandpass filters was angled tuned to 2 degrees to ensure the maximum transmission for the quantum dot sample with the three filters in place.

The quantum dot was non-resonantly optically excited using a 784 nm PicoQuant LDH series pulsed semiconductor diode with a 90 ps temporal response. Resonant excitation into the first excited state (s-shell) in a quantum dot results in a lower $g^{(2)}(0)$ value due to electron-hole pairs being created within the dot [31] however a tuneable laser at this

wavelength was not available. A custom microscope shown in Figure 3.8 allowed the sample to be optically excited and allowed the emitted light to be collected.

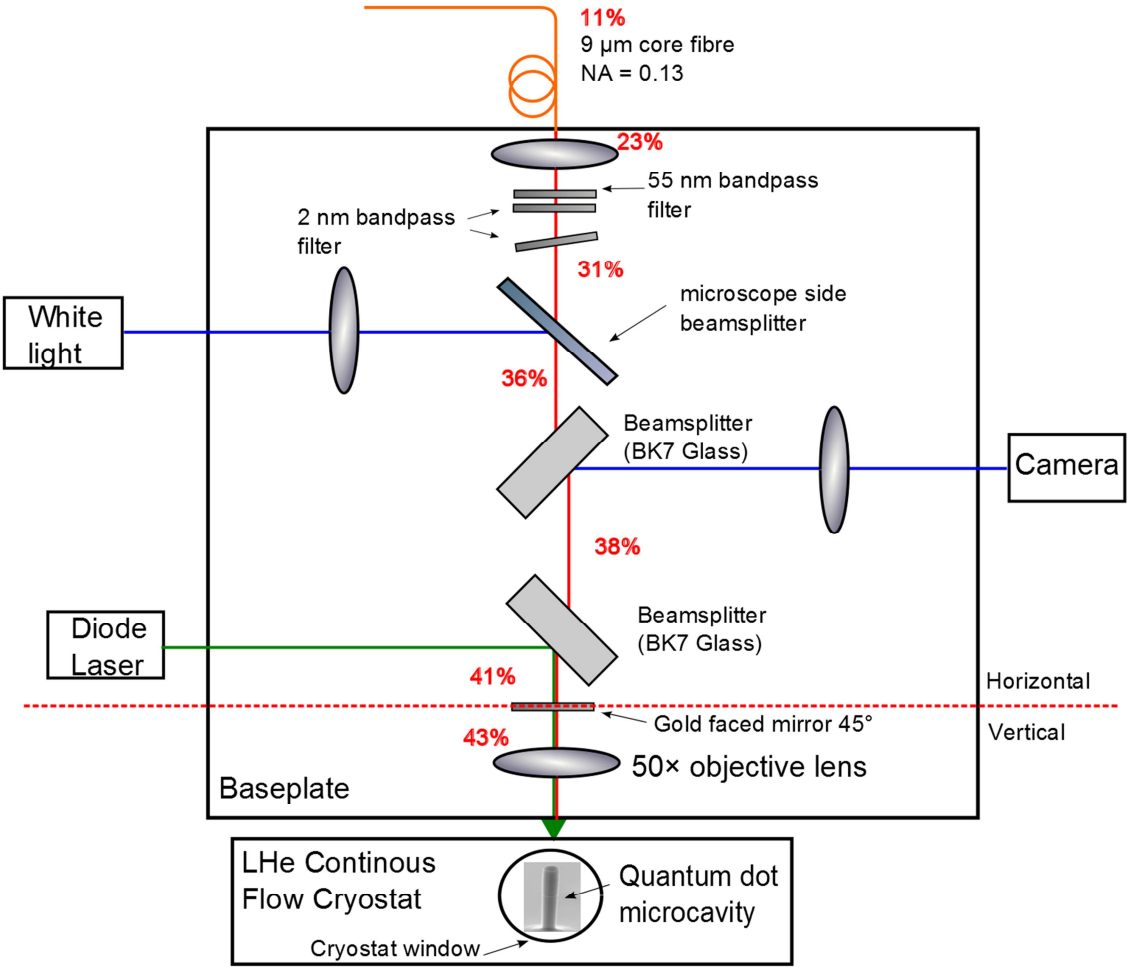

Figure 3.8. Diagram showing the microscope used with the quantum dot microcavity. The imaging optics are on a moveable (x-y plane) baseplate and the cryostat was held fixed below. The white light source and the camera provide the ability for course alignment and sample identification. The excitation laser diode at a wavelength of 784 nm is reflected off the BK7 beamsplitter and the gold face mirror to the sample through the 50× objective lens. Photons emitted from the sample were collected by the objective lens (NA=0.42) and coupled into the 9 µm core diameter fibre. The transmission at each stage of the microscope relative to the cryostat window is shown numerically in red.

The microscope system operated in an infinite conjugate system which allowed the easy addition of beamsplitters or mirrors into the optical path. An infinity corrected Mitutoyo 50× objective with a numerical aperture (NA) of 0.42 was used to collect light from the sample and also to focus the excitation laser onto the sample. The light collecting ability of the lens is given by

$$NA = n\sin\theta \approx n\frac{D}{2f} \qquad \text{Equation (3.5)}$$

where n is the refractive index, D is the entrance pupil diameter and f is the focal length. The higher the NA value the more photons emitted from the quantum dot microcavity that can be collected by the lens. The objective lens was mounted in a three axis piezo-electric motor stage with sub nanometre resolution [32]. The white light source and camera system was used for sample identification and for rough alignment purposes. The excitation diode laser, operating at a wavelength of 784 nm is focused onto the sample by first reflecting off a BK7 glass beamsplitter and then is reflected 90 degrees from this plane by a gold-face mirror via the 50× objective, through a glass window in the cryostat and onto the sample. A gold mirror has the advantage of having one of the highest relativities of metals in the infrared and has a flat spectral response [33]. The objective lens has a long working distance of 13 mm which allowed light to be focused through the cryostat window and onto the sample which lay beneath.

A 9 μm core diameter collection fibre mounted on a three axis piezoelectric micropositioner allowed the light emitted from the sample to be used for characterisation or for use in the QKD experiment. A 9 μm core fibre offered the best compromise of maximum collection efficiency while at the same time ensuring good spatial filtering of unwanted cavity modes. To ensure optimal alignment of the collection fibre a laser with a similar wavelength to the emission from the quantum dot was coupled into the fibre and the three axis piezoelectric micropositioner was adjusted until the laser spot was in a sharp focus in the same position as the excitation laser. To evaluate the coupling efficiency of the microscope a laser with an identical wavelength to the emission from the quantum dot was transmitted through the microscope. It was determined that of the photons emitted from the microcavity that were successfully captured by the microscope objective, 11% were coupled successfully into the 9 μm core fibre shown in Figure 3.8. The cryostat was maintained at a pressure of about 2×10^{-6} mbar (0.2 mPa) to ensure that contaminants (including the ambient air) in the chamber did not freeze or condense onto the sample when operated at low temperatures. This was achieved by using a rotary vane vacuum pump and a turbo pump. The quantum dot samples were placed onto the coldfinger of an Oxford Instruments CF-1104 cryostat [34]. The continuous flow cryostat can be cooled by liquid nitrogen or liquid helium depending on the required temperature of operation. When the cryogen

evaporates in the cryostat it is continuously replenished by a steady flow from a storage dewar. The temperature inside the cryostat can be maintained at the desired level by controlling the flow rate of cryogen into the cryostat together with using a heating element controlled by a proportional–integral–derivative (PID) feedback loop. The cryostat had its thermal heat shield removed to allow optical excitation of the quantum dot which meant that temperatures of 80 K could be achieved using liquid nitrogen (LN_2) or 26.7 K using liquid helium (LHe). This can place a restriction on the narrowest spectra linewidth that is achievable as it was shown experimentally elsewhere that the spectra linewidth can increase with increasing temperature due to exciton–phonon interactions [35]. The ability to not only stabilise the temperature but also to controllably alter it is very important in order to tune the quantum dot emission with the microcavity resonance. As the temperature of the system is increased the wavelength of emission from the quantum dot increases as does the wavelength of the cavity mode. However the cavity mode increases at a slower rate than the quantum dot thereby allowing the quantum dot to be brought into resonance with the cavity [36]. The cavity mode emission wavelength increases due to temperature dependence of the refractive index while the quantum dot emission shifts due to the temperature dependence of the bandgap [37]. It is also possible in general to tune the quantum dots by the quantum Stark effect which allows the wavelength of emission to be tuned over a wider range [38]. The quantum dot can be placed between a metallic contact and a Schottky barrier. The gate voltage induces a vertical electric field which shifts the exciton energy through the Stark effect [39].

3.5 Characterisation of quantum dot micropillar samples

The spectral characteristics of the quantum dot were analysed using a triple grating monochromator (Acton SpectraPro 2500i, 0.05 nm resolution) using a liquid nitrogen cooled front illuminated charged coupled device (CCD) camera with a dark count rate of 750 count/s per pixel. The triple grating offers good spectral resolution in the infrared [40] but does have the drawback of having less throughput. The monochromator had an internal swing mirror than allowed the light reflected from the grating to be imaged onto the CCD camera or to be coupled into a fibre. When used as a tunable filter the resolution of the monochromator is determined by the collection fibre core diameter. The effect of temperature tuning the quantum dot in and out of resonance with the cavity is shown in Figure 3.9. Emission from the cavity mode is evident at a temperature of 24.8 K when the dot is not resonant with the cavity.

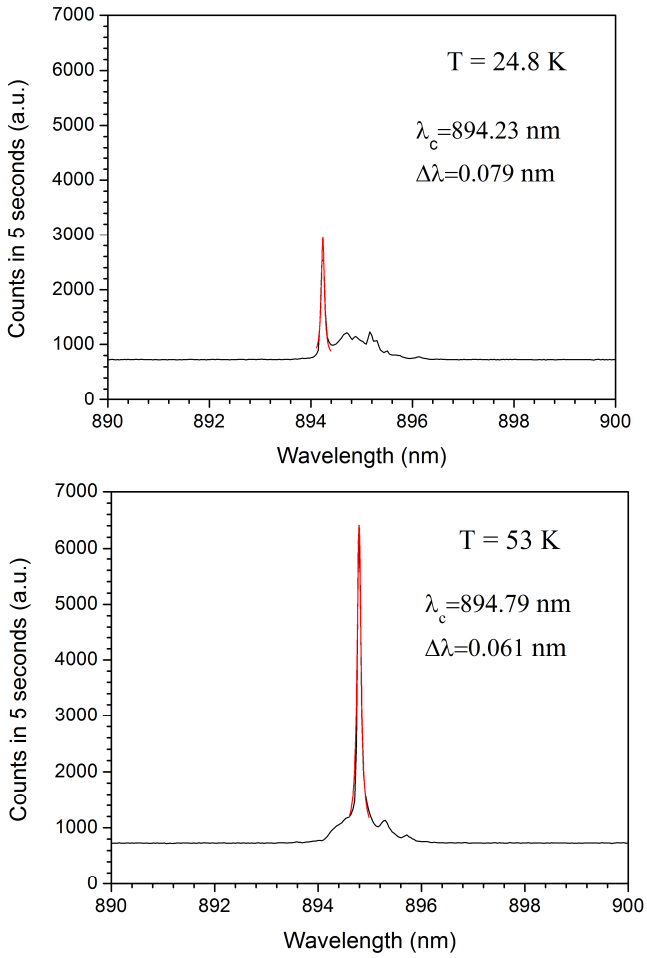

Figure 3.9. The top graph shows the spectra obtained at 24.8 K when the quantum dot is out of resonance with the cavity while the bottom graph shows the spectra obtained at resonance at a temperature of 53 K. An increase in the intensity was observed when the quantum dot was tuned into resonance with the cavity, an effect which was also observed in Ellis et al [41]. The Q factor of the micropillar was estimated to be ~14000 using $\lambda/\Delta\lambda$ [42]. The linewidth was determined using a Lorentzian function fit.

By temperature tuning the dot from off resonance at 24.8 K to on resonance at 53 K the central wavelength shifted from 894.23 nm to 894.79 nm ($d\lambda/dT =$ 0.01985 nm/K) with a reduction in the linewidth from 0.079 nm to 0.061 nm. The quality factor Q (a measure of the time a photon is trapped in the cavity) of the device can be estimated by the ratio of the central wavelength λ to the linewidth $\Delta\lambda$. The Q factor was calculated to be 14668 using these values when the QD is at resonance with the cavity. The Purcell factor can be related to the Q factor by Equation (3.2). It can be seen from this equation that there is a definite advantage to having a cavity with a higher Q

factor. The Purcell effect predicts an increase in the spontaneous emission rate from an atom when it is in resonance with a cavity. In Figure 3.9 an increase in intensity is observed when the dot is on resonance at 53 K. The integrated count in the peak increases by a factor of ~2.2 when the dot is on resonance compared to the off resonance case.

Figure 3.10 shows the spectra obtained from the quantum dot when only using a single 55 nm width bandpass filter.

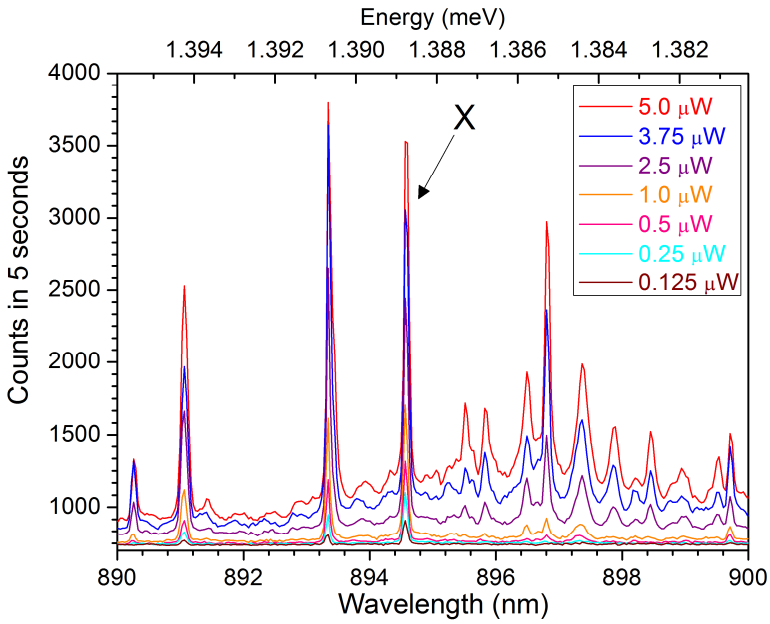

Figure 3.10. Spectra of the quantum dot at various excitation powers measured at the cryostat window using a 55 nm bandpass filter. The transition marked X was the emission that was chosen for the QKD measurement, centred on 1.3885 eV or 893.6 nm. The temperature was maintained at 53 K to ensure the dot was in resonance with the cavity.

Several distinct emission peaks, which is a feature of non-resonant excitation, are evident resulting from the fact that more than one quantum dot is being excited with each one having slightly different emission characteristics due to the Stranski-Krastanov growth process and also biexciton transitions [12]. As the excitation power is increased the emission from the cavity mode also increases which results in a higher baseline in the emission spectra due to emission from the wetting layer. The quantum dot which has an emission at 894.5 nm was chosen as the best candidate as it gave the best $g^{(2)}(0)$ values over the range of excitation powers as shown in Figure 3.15. Although the peak height appearing at a wavelength of 893.3 nm is larger the integrated photon flux is

comparable and the main advantage is seen at the lower excitation power levels where the peaks at 895 nm are about 10% higher than at 893.3 nm.

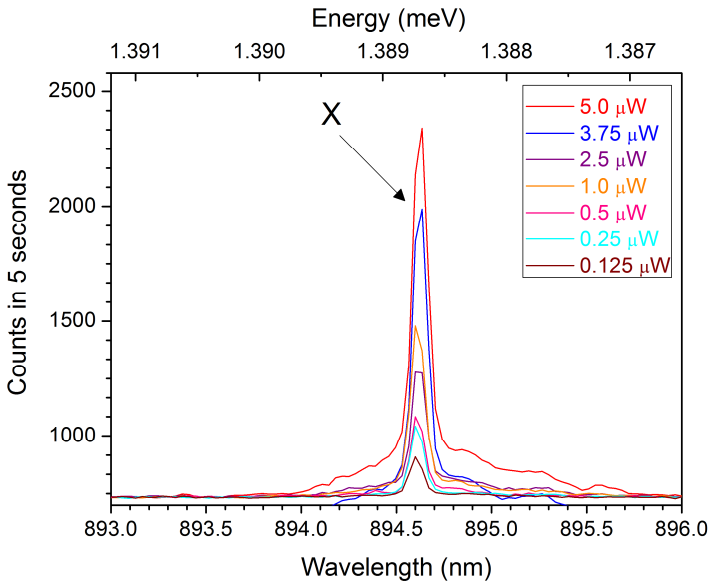

Figure 3.11. Spectra from quantum dot source with two 2 nm bandpass filters. The central wavelength was 894.66 nm (1.387 eV), with a spectra FWHM of 0.086 nm. The sample was maintained at a temperature of 53 K to ensure the dot was in resonance with the cavity.

Figure 3.11 shows the spectra obtained from the quantum dot source with the combination of the 55 nm bandpass filter and two 2 nm narrow bandpass filters. The additional emission peaks evident in Figure 3.10 have been eliminated and the emission from a single quantum dot transition was obtained. The spectral FWHM was measured to be 0.086 nm (0.165 meV) and showed no obvious trend with increasing excitation. The homogenous linewidth of the fundamental transition in InAs/GaAs quantum dots at low temperatures (< 10 K) ranges between a few μeV for resonant pumping [43] and a few 10's of eV when increasing the energy detuning between optical excitation and the optical fundamental transition. The measured linewidth of 0.86 nm is not resolution limited by the spectrometer and its relatively large FHWM indicates that broadening could be caused by either acoustic phonons which becomes more important at higher temperatures [44] [45] or that emission from an ensemble of other quantum dots could be contributing to the broadening [46]. Quite often in order to identify whether an exciton or biexciton is responsible for a particular emission line, the integrated PL intensity is plotted as a function of the laser power [47]. Figure 3.12 shows a typical log-log plot showing the photoluminescence (PL) integrated intensity dependency on

the laser excitation power. As is quite commonly observed under low excitation powers, a PL intensity which shows an almost linear dependence on the pump power (P), $I_X \propto P^1$, indicates a recombination due to an exciton whereas a quadratic dependence, $I_{X_2} \propto P^2$, indicates a biexciton recombination. Since it takes two electron-hole (e-h) pairs to form a biexciton (two-photon excitation), the emission intensity of the biexciton to exciton transition depends nonlinearly on the excitation intensity whereas an exciton is formed in a dot primarily by directly capturing one e-h pair, the emission intensity of the exciton recombination depends linearly[6]. Figure 3.12 shows an exciton PL intensity which is proportional to $P^{0.72\pm0.02}$ with the uncertainly determined by a least square fitting. Santori *et al.* [48] and Pelton *et al.* [15] also using InAs quantum dots in a micropillar cavity achieved counts rate of the order of ~200k counts/s in comparison to about 2500 counts/s achieved here at the highest excitation power shown in Figure 3.12.

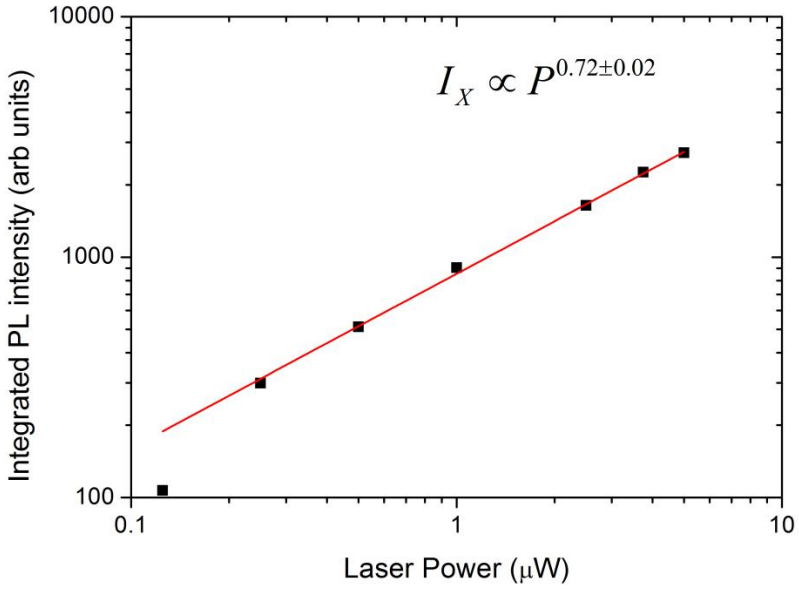

Figure 3.12. Log-log plot of the integrated PL intensity against pump power for the X transition. The almost linear dependence of the PL intensity on the laser pump power suggests an exciton recombination process.

The experimental setup for the measurement of the second order cross correlation function $g^{(2)}(0)$ is shown in Figure 3.13. The implementation uses the Hanbury Brown-Twiss experiment described earlier. The detector events registered on the single-photon avalanche photodiodes (SPAD) are recorded on a Becker and Hickl SPC-600 time-correlated single-photon counting (TCSPC) card and are used as the stop and start for the timer.

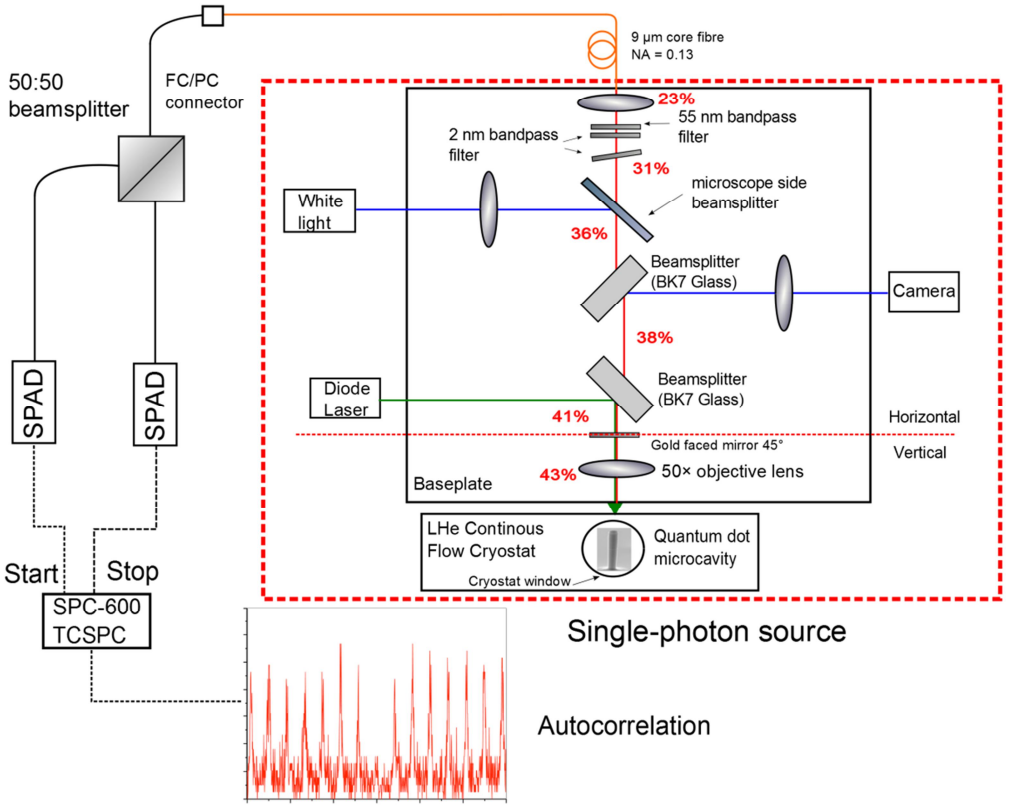

Figure 3.13. Experimental apparatus to perform the second order autocorrelation function. The experiment is implemented using the Hanbury Brown Twiss approach. The dashed red box denotes the single-photon source elements.

Figure 3.14 shows a typical autocorrelation measurement performed on the emission line of interest from the dot within the 1 µm diameter pillar. The excitation pulse repetition rate is 40 MHz, wavelength 784 nm and excitation power is 1 µW. The count rate on each detector was ~2000 counts/sec and 6450 coincidence counts were recorded in a 150 integration time. The value for $g^{(2)}(0)$ can be calculated by the summation of the normalised counts in the single-photon peak at $\tau = 0$ divided by the total counts in the multi- photon peaks [49]. The peaks were fitted with a Lorentzian and the total counts within a 3ns FWHM were taken. The variation in $g^{(2)}(0)$ as a function of the excitation power on the sample surface is shown in the main graph in Figure 3.16. The insert graph shows the variation in the count rate outside the Lorentzian fit as a function of the excitation power on the sample surface. The increase in $g^{(2)}(0)$ may be due to other quantum dots which can feed the cavity. It has been shown elsewhere [50], [51] that when a single QD is isolated the cavity emission can be antibunched as well. At higher pump rates additional spectral lines can emerge, associated with multi-exciton transitions from other dots which can add to the background signal [52].

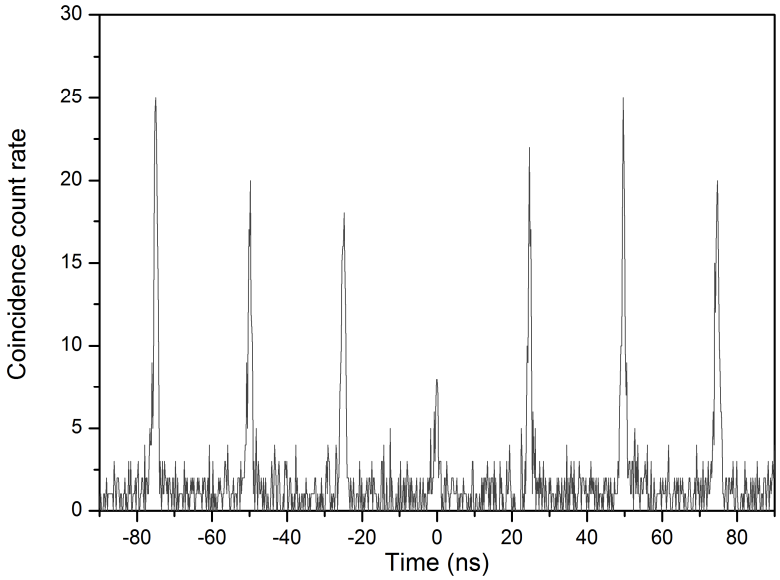

Figure 3.14. Autocorrelation measurement on the 1 μm diameter pillar quantum dot under an excitation power of 1 μW measured at the cryostat window. The count rate recorded on each SPAD was ~2000 counts/s. The repetition frequency of the laser is 40 MHz. Peaks are observed at $n \cdot \tau_{rep}$ *where* τ_{rep} *is the laser repetition rate and* n *is an integer value. The total coincidence count was 6450 in a 150 minute acquisition time.*

Figure 3.15 shows the photon flux leaving the single photon source measured at the 9 μm core diameter output fibre shown on the left axis. The right hand axis shows the estimated photon flux accepted by the microscope assuming an 11% coupling efficiency of the microscope and a detector efficiency of 35%. The maximum recorded photon flux was about 4 MHz corresponding to an excitation power of 5 μW but results in a relatively high $g^{(2)}(0)$ value of 0.85. The lowest excitation power of 0.25 μW resulted in a photon flux of 200 kHz and a $g^{(2)}(0)$ value of 0.32. An upper bound on the probability to generate two or more photons in a given pulse can be given by

$$P(n \geq 2) = \frac{\mu^2}{2} g^2(0) \qquad \text{Equation (3.6)}$$

where μ is the mean photons per pulse[53]. A $g^2(0)$ of 0.85 and 0.32 reduces the multi-photon probability to ~4.25% and ~1.6% respectively compared to a weak coherent pulse with $\mu = 0.1$. Using background subtraction techniques [54] the $g^2(0)$ at the highest excitation power was reduced to 0.74 and at the lowest excitation power was reduced to 0.21.

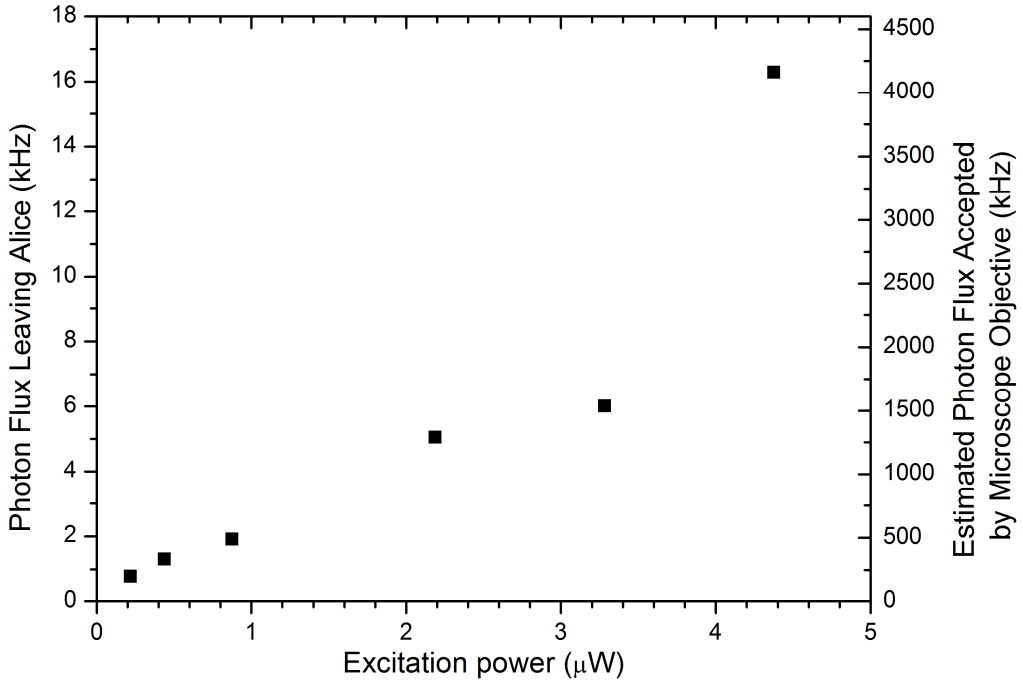

Figure 3.15. The left-hand axis shows the photon flux which exits Alice as a function of the excitation power at the sample surface. The right-hand axis shows the estimated photon flux emitted from the microcavity into the acceptance cone of the microscope objective assuming 35% detection efficiency for the Si-SPAD and an 11% coupling efficiency in the microscope.

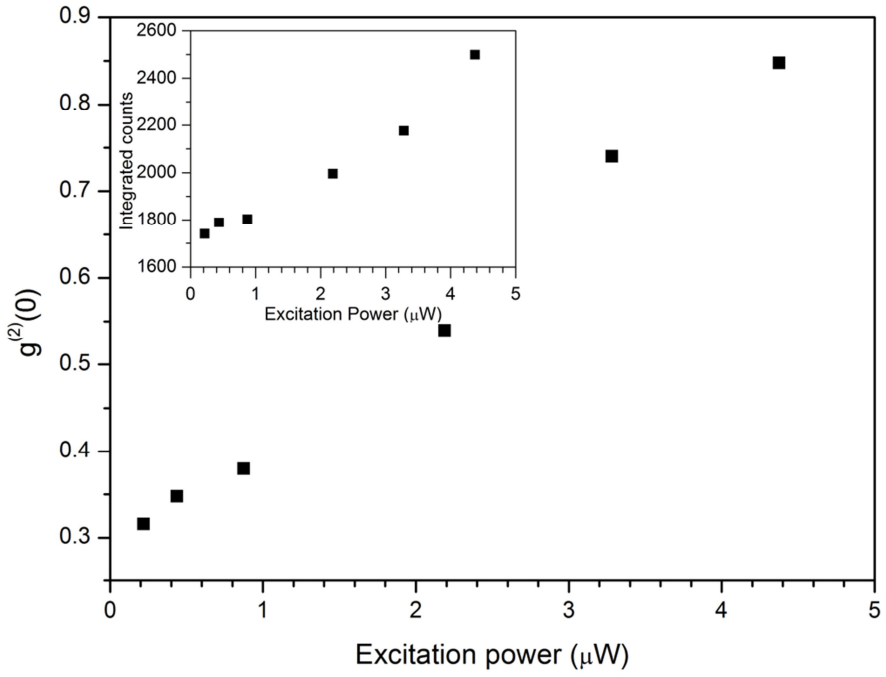

Figure 3.16. The main graph shows the variation of $g^{(2)}(0)$ as a function of the excitation power at the sample surface. The insert shows the integrated count rate obtained outside the peak area as a function of the excitation power. The laser pulse repetition rate was 40 MHz.

In order to estimate the efficiency of the single photon source when measured at the first collection lens, the number of emitted photons divided the number of incident photons incident on the 1 μm diameter pillar was calculated. The beam diameter of the collimated excitation laser was ~4 mm, which when assuming diffraction limited optics, gave a spot size of 0.9 μm using the 0.42 NA microscope lens (spot size $\approx 1.22\lambda/NA$ [55]). Using this approach the source efficiency was estimated to be less the 1%.

Figure 3.17 shows a time resolved photoluminescence trace (TRPL) of the quantum dot at an excitation power of 1 μW which show an emission lifetime of 464 ps. An iterative reconvolution technique [56] is used to measure the primary photoluminescence lifetime of the sample. The output of a linear system for an input $F(t)$ and a detector instrumental response $I(t)$ is given by the convolution integral

$$G(t) = \int_{\tau=0}^{t} F(\tau) I(t-\tau) d\tau \qquad \text{Equation (3.7)}$$

where the instrumental response $I(t)$ is the instrument output for a delta function input at $t = 0$ and $G(t)$ is the output data [57]. Both $G(t)$ and $I(t)$ are known and the decay function of the quantum dot, $F(\tau)$ is calculated by deconvolution. The data analysis program (Edinburgh Instruments T900) performs this deconvolution and fits $F(t)$ using two exponential decays. The emission lifetime recovered at the highest excitation power of 5 μW was 563 ps, which ensures the dot has fully relaxed before the next excitation pulse. The radiative lifetime is characterised by the carrier capture and relaxation process in the quantum dot. Carriers are injected into the GaAs matrix surrounding the dot. These carriers are then captured via the wetting layer into the quantum dot and rapidly relax to the ground state [6]. An electron and a hole, which have spins which are antiparallel, results in an optically allowed transition and is referred to as a bright exciton. It has a total angular momentum projected into the QD growth axis of $J_z = \pm 1$. If the spins are parallel it leads to the formation of a dark exciton with $J_z = \pm 2$ which is optically forbidden. The TRPL trace is characterised by a double exponential, the fast component comes from the recombination of a bright exciton while the slower decay tail may be due to the presence of a dark exciton state. Emission from a dark state is eventually possible by the exciton scattering into a bright exciton by either the spin-flip of either the hole or electron [58]. An attempt to characterise the

polarisation dependent spontaneous emission was prevented as reflection off the gold faced mirror scrambled the polarisation information.

Using the radiative lifetime of 563 ps when optically pumped at 5 µW and the estimated photon flux captured by the collection lens the collection efficiency was estimated to be about 0.185%. Other optically pumped microcavity pillar devices have reported efficiencies of ~40% [59] [60]. The low efficiency of the quantum dot in this chapter may be due to a combination of the generation of dark states which is a dipole forbidden transition and can limit the maximum achievable emission rate, a mismatch in the overlap between the emitter transition dipole and the electric field of the cavity mode, given by the third term in Equation (3.2) or due to losses in the top mirror of the DBR.

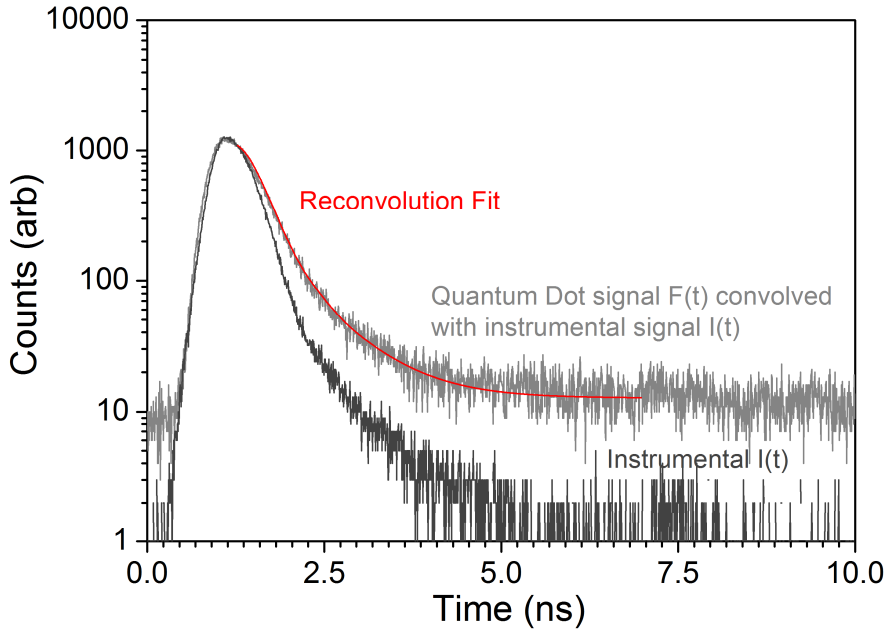

Figure 3.17. The time resolved photoluminescence (TRPL) trace $F(t)$ of the quantum dot with an excitation of 1 µW is shown. An iterative reconvolution technique [56] is used to measure the primary photoluminescence (PL) lifetime of this sample, the reconvolution trace is shown in red. The PL lifetime was measured to be 464 ps. The detector instrument response $I(t)$ is also shown.

3.6 Quantum key distribution with a single photon source

3.6.1 Overview of system

The single-photon source which has been described in the previous sections is used to implement the BB84 protocol for quantum key distribution using polarisation encoding on the photons. A free space polarisation modulator (Newport 4102 NF broadband

polarisation modulator) is used to produce the four polarisation states for the BB84 protocol using vertical and horizontal polarisation encoding for one basis set and left and right circular polarisation for the other basis set. The polarisation modulator works by the electro-optic effect. When an electric field is applied across an optical medium the refractive index of the medium changes anisotropically [61]. This optic-electric effect can introduce new optic axes into naturally refracting crystals or to make naturally isotropic crystals doubly refracting. The change in refractive index Δn due to an applied electric field E_z in the z direction is given by

$$\Delta n = \frac{n_0^3}{2} r E_z \qquad \text{Equation (3.8)}$$

where r is the linear electo-optic coefficient and n_0 is the refractive index. The device operates when an optical beam, which is polarised at 45° to the crystal's principle axis, propagates parallel to the crystals optic axis. When there is no applied electric field the crystal acts as a retarding waveplate. When an electric field is applied, the electro-optic effect changes the indices of refraction along the two crystal directions by different amounts, which changes the retardation of the waveplate. The optical layout shown in Figure 3.18 forms a Pockel's electro-optic modulator and is used for the results shown in Figure 3.21.

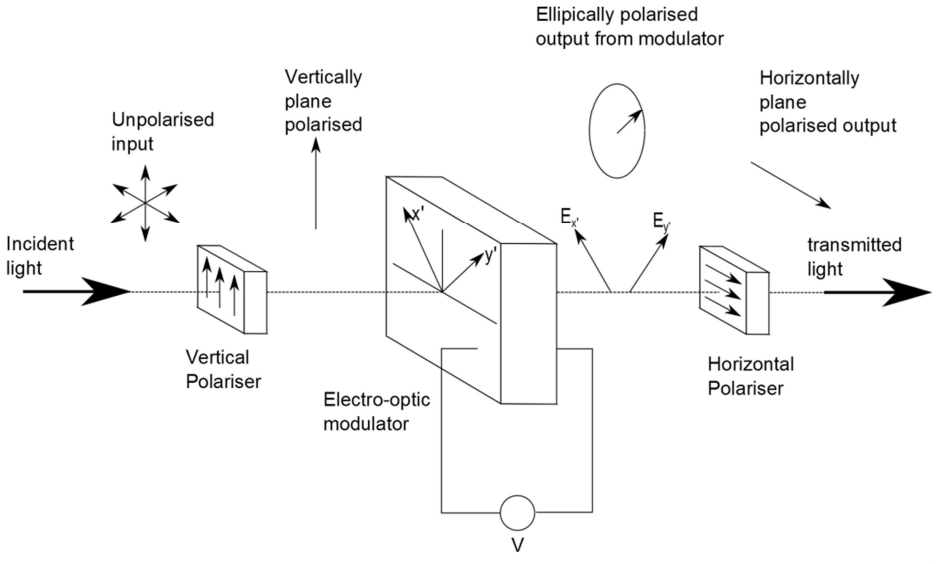

Figure 3.18. Components of a Pockels electro-optic modulator. The modulator is placed between crossed polarisers. The crystal acts as a variable waveplate which changes the polarisation of the output beam from linearly polarised to circular, to linear to circular etc. as the applied voltage is increased which controls the amount of light that is finally transmitted [61].

A high extinction ratio input polariser (10000:1) guarantees that the unpolarised output from the quantum dot [27] is polarised at 45° to the crystal's principal axes. The crystal acts as a variable waveplate, changing the exit polarisation from linearly polarised (0° rotated from the input) to circularly polarised, to linearly polarised (90° rotated), to circular, etc., as the applied voltage is increased. As in the case of Figure 3.18, when the modulator crystal is placed between crossed polarisers the transmitted intensity I is given by

$$I = I_0 \sin^2\left(\frac{\pi}{2}\frac{V}{V_\pi} + \phi\right) \qquad \text{Equation (3.9)}$$

where V_π is the voltage required for a phase retardation of π, V is the applied voltage on the crystal and ϕ is the phase. The polarisation modulator required that the input optical beam had a maximum diameter of 500 µm across the entire 56 mm length of the crystal [62]. The optical arrangement to achieve this is shown in Figure 3.19. For the launch optics a 16 mm focal length lens (f_1) is used to collimate the photons emitted from the 9 µm core diameter fibre from Alice and a 500 mm focal length lens (f_2) is used to focus the photons through the modulator. The collection optics comprises of one 300 mm (f_3) and one 8 mm (f_4) focal length lens. The loss of the launch/collection optics and the modulator was 9.5 dB.

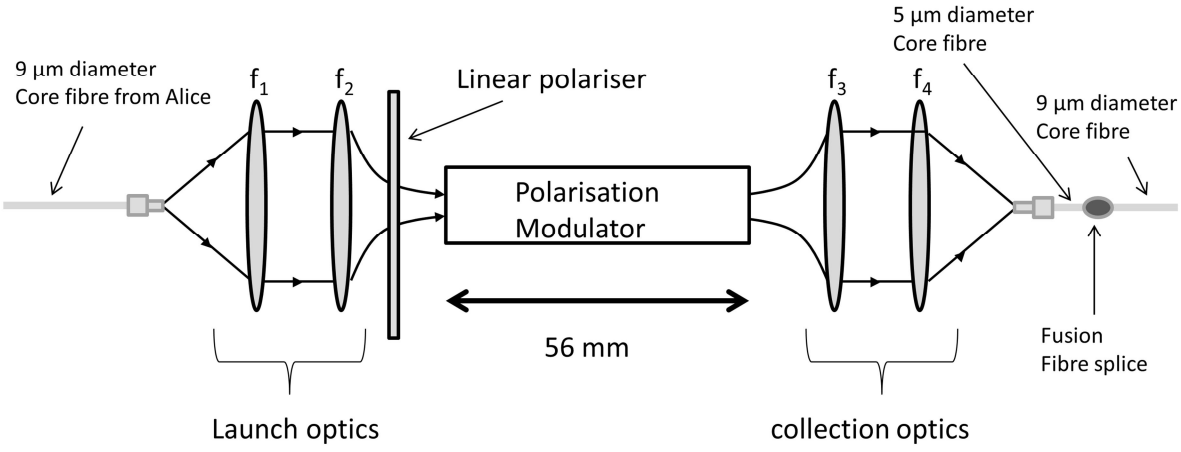

Figure 3.19. Optical layout to ensure the maximum beam width across the polarisation modulator is 500 µm. The loss of this stage including the collection loss into the 9 µm diameter core fibre is 9.5 dB.

The Newport 4102 NF broadband polarisation modulator containing a crystal of $LiNO_3$ is a resonant device which operates at a clock frequency of 40 MHz which limited the maximum clock rate in the experiment. The crystal is part of a resonant LCR circuit which ensures that energy is efficiently transferred to the crystal and is not lost across

the internal resistance, R, of the modulating source. The inductance L is chosen such that $4\pi^2 f_0^2 = 1/LC$, where f_0 is the modulation frequency. This enables crystals with lower values of V_π [61]. The driving electronics for the crystal allows an external analogue voltage (0 to 5V) to modulate the output RF level. Figure 3.20 shows the gain curve for the Newport (Model 3363) resonant modulator driving electronics. A pulse pattern generator provided the input voltage signal. The polarisation modulator can be driven at a maximum of 25 V (peak to peak) [62] which is an issue when trying to produce the final fourth polarisation state for BB84. Figure 3.21 shows how the transmitted optical power varies with the applied voltage when the polarisation modulator is placed between crossed polarisers similar to the arrangement in Figure 3.18. In Figure 3.21 it is possible to see that the first linear state occurs at 0 V, the first circular occurs at 9.6 V indicated by the 50% transmission and the second linear at 17.67 V. The voltage which is required to generate the second circular state is predicted to occur at 27.27 V which exceeds the maximum safe driving voltage for the crystal and also exceeds the maximum output of the modulator driving electronics. This means that the polarisation modulator is unable to provide the four polarisation states for a fully working implementation of the BB84 system.

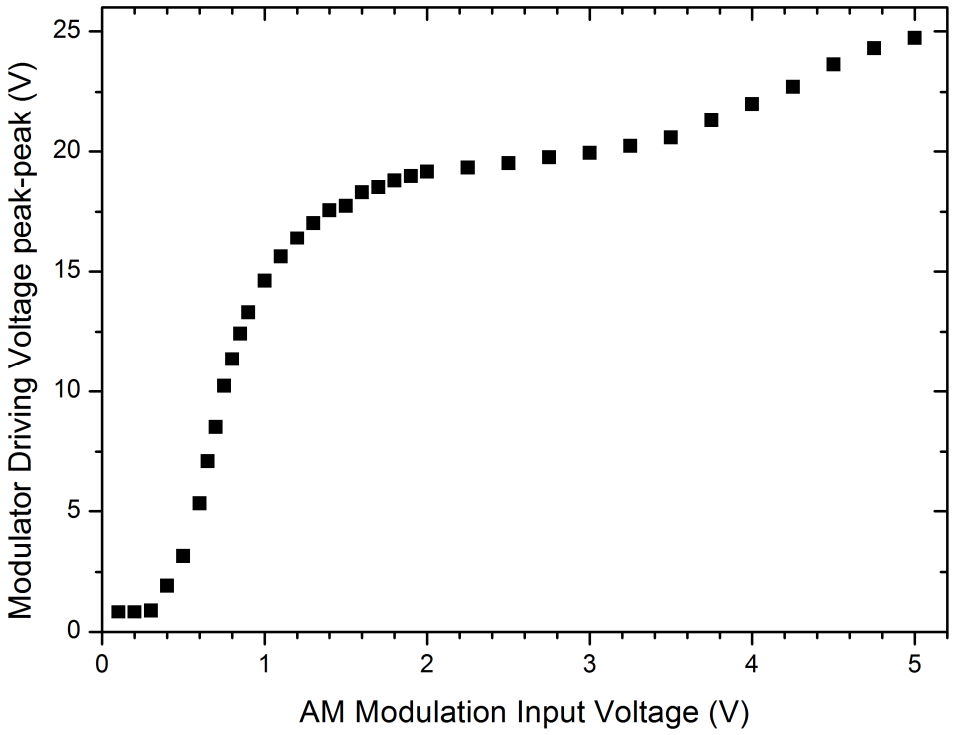

Figure 3.20. The gain curve for the amplitude modulator driving electronics.

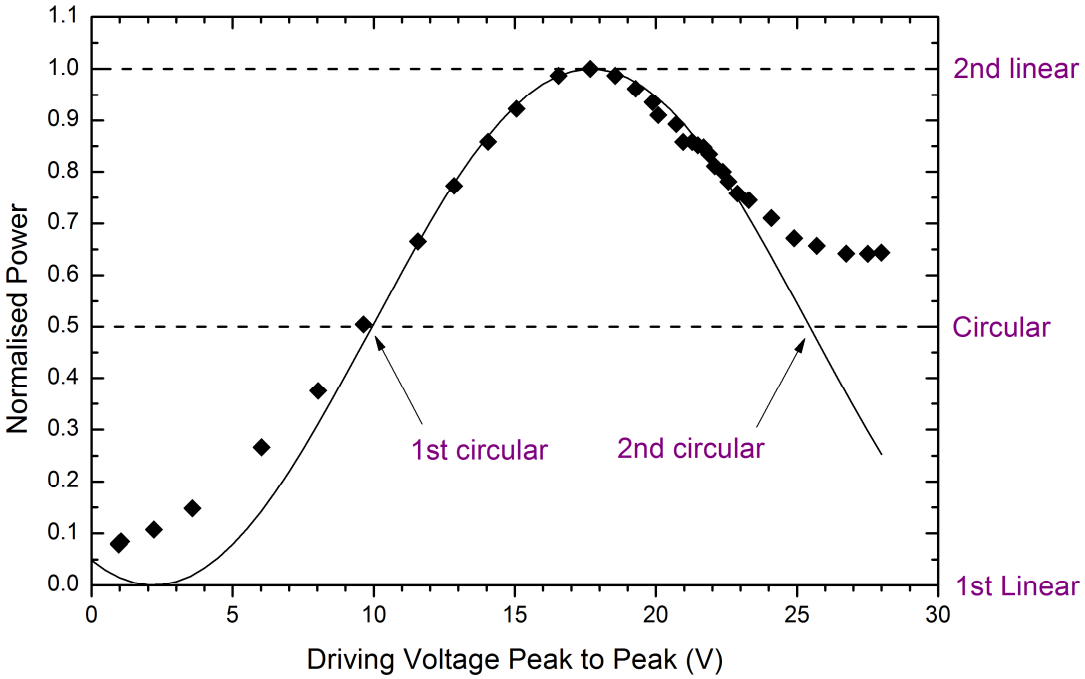

Figure 3.21. Shows the normalised power measured at the output of the polarisation modulator after passing through an analyser polariser. The analyser is orientated such that when there is zero applied voltage the transmitted intensity is zero. The two linear states are achieved at a driving voltage of 0 and 19.67 V. The first circular state occurs at 9.6 V indicated by 50% transmission. After obtaining maximum transmission the transmitted power never decreases to 50% again indicating that the second circular state is not achievable. The expected power is obtained using Equation (3.9).

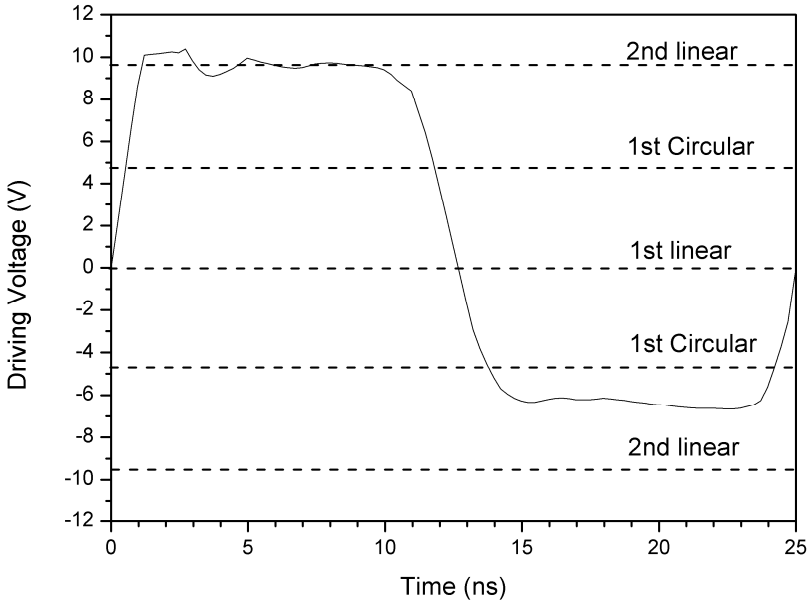

Figure 3.22. One period of the electrical driving signal to the polarisation modulator to generate the 4 states. A DC offset means that while the second linear state is achievable in the first half cycle it is not obtainable in the second half cycle.

Figure 3.22 shows a typical period of the electrical driving signal for the polarisation modulator. It becomes obvious from the figure that while the first linear, first circular and second linear voltage levels are achievable on the first half cycle of the wave the second linear is not achievable on the second half due to the DC offset in the electrical signal. In theory a bias Tee, which adds a DC offset to an AC source, could have been inserted into the electrical circuit to compensate for this offset but the additional electrical loss induced and electrical ringing issues made this impossible.

It is necessary to synchronise the optical light pulse travelling through the polarisation crystal with the electrical signal driving the crystal to ensure that the light pulse is modulated with the correct polarisation state. To achieve this, the electrical signal used to pulse the laser is delayed with respect to the modulator signal. A schematic of the experiment is shown in Figure 3.23.

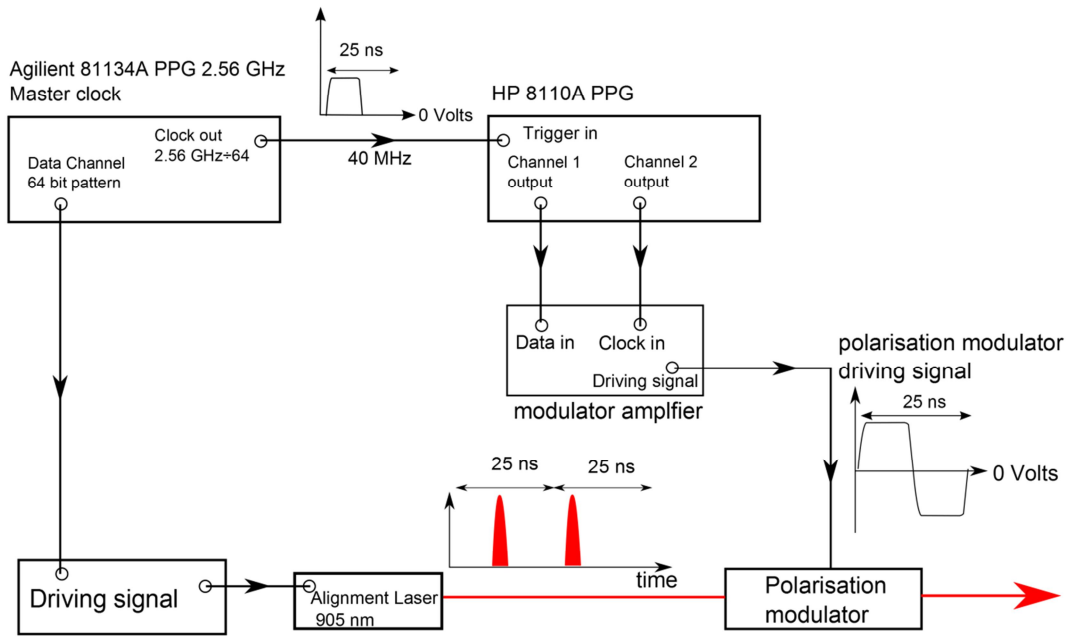

Figure 3.23. Experimental arrangement to synchronise the optical light pulse travelling through the polarisation crystal with the electrical signal driving the crystal to ensure that the light pulse is modulated with the correct polarisation state. The Agilent 811134A PPG is used as the master clock for the system and drives the laser driver with a 64 bit data pattern at 40 MHz. The HP 8110A PPG, which is clocked by the master clock frequency divided by 64, is used to drive the modulator driver.

The Agilent 81134A pulse pattern generator (PPG) is used as the 2.56 GHz master clock in the system. The output is frequency divided by 64 to provide the 40 MHz clock input for the HP81110A PPG. This HP81110A PPG is capable of outputting

larger amplitude signals and is used to provide the source for the modulator internal oscillator and also the AM modulation input. The laser is triggered by the data output channel on the Agilent 81134A PPG, which is a 64 bit pattern that repeats every 25 ns and whose electrical width is 390.625 ps. It is evident from Figure 3.21 that linear polarisation modulation is only achievable over a limited operating range. This results in the polarisation states in Figure 3.24 being unequally spaced in time. To compensate for this the laser has to be pulsed non-periodically to coincidence with the polarisation states produced by modulator. This has security implications as an eavesdropper can measure the time interval between pulses to gain full information about the states.

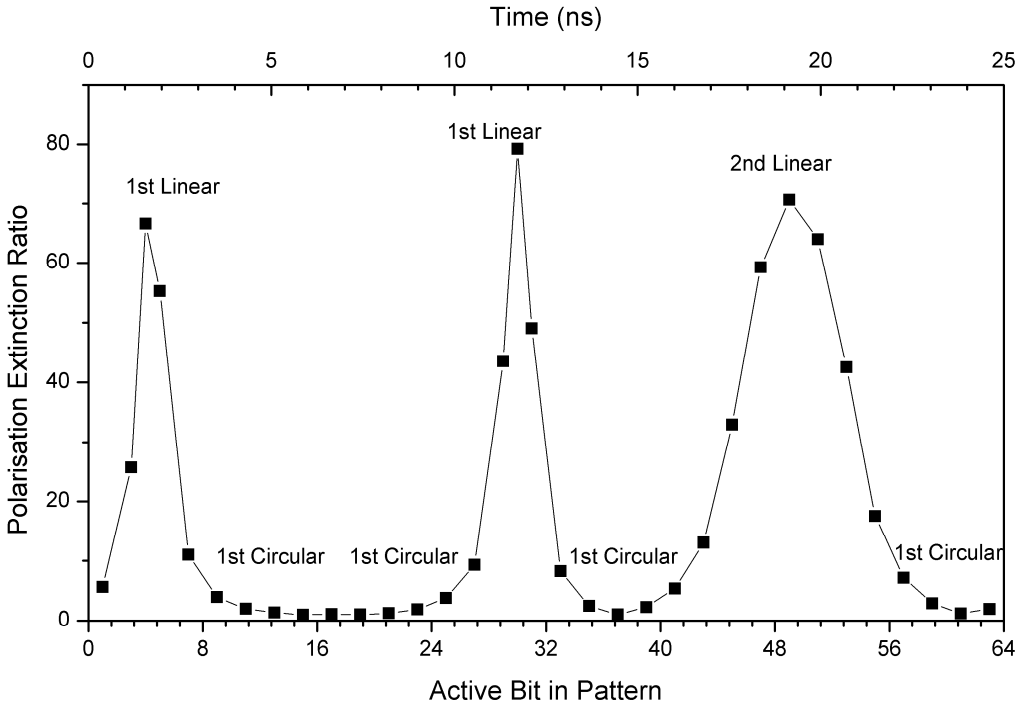

Figure 3.24. The variation in the polarisation extinction ratio is plotted as the active bit in a 64 bit pattern, which is used to trigger the laser is swept across one period of the 40 MHz clock signal for the modulator.

The diagram shown in Figure 3.25 shows the outline of the test bed for the implementation of the BB84 protocol. The polarisation encoding system which includes the polarisation modulator in Alice and the beamsplitter, polarisation beamsplitters (PBS) and static polarisation controllers (SPC) in Bob was a relatively uncomplicated system to build and to more importantly to maintain its alignment. For example the SPC in Bob needed adjustment to correctly align the polarisation with the PBS but this was found to remain stable for at least a day. If a phase encoding system was employed using fibre interferometry, active and more frequent feedback is required to ensure path length changes in the arms of the interferometer is minimised. The

importance of the stability of the polarisation encoding system can be understood when considering the alignment of the optical components that make up the single-photon source (SPS). The SPS system required much more frequent adjustment to ensure the highest photon flux was achieved and therefore having an encoding system which had a stable alignment made data acquisition easier. A PicoQuant LDH series excitation diode laser at 784 nm, operating at 40 MHz, excites the quantum dot sample through the custom microscope. The emitted light at a wavelength of 904.5 nm is collected by the microscope and focused through the polarisation modulator which sets the polarisation state of the light. Two orthogonal linear states were used in the course of the experiment. These states occur at bit positions 30 and 50 in Figure 3.24. The pulse pattern generator then outputted a 128 bit pattern with bits 30 and 114 active (one period of 64 bits + 50 in the next). This ensures that a laser pulse train is created which has a mean frequency of 40 MHz. The light then travels through standard telecommunications fibre to Bob. To ensure the light propagates in the fundamental mode short lengths of 5 µm diameter core fibre are spliced onto the ends of the 9 µm fibre which removes higher order longitudinal modes which is a form of spatial filtering [63].

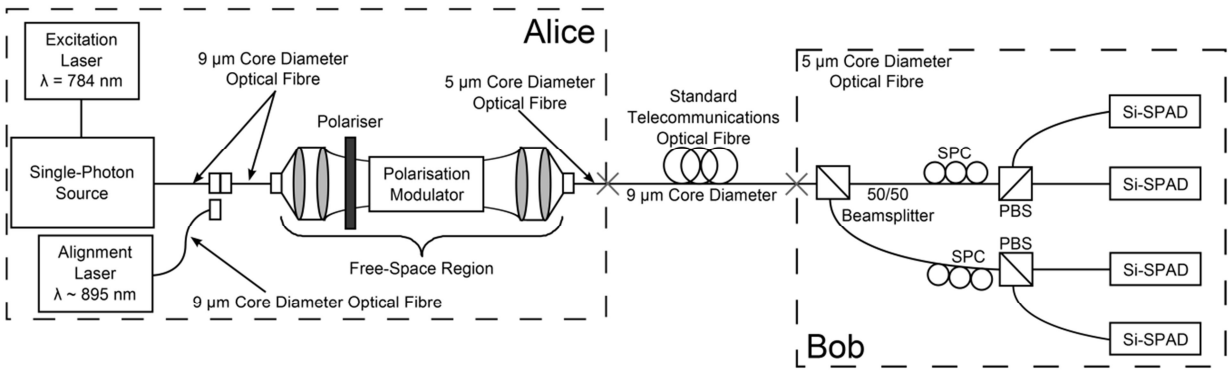

Figure 3.25. Schematic diagram of the QKD system. The box labelled "single-photon source" contains the custom microscope used to optically excite the quantum dot and to collect its emission. The quantum channel is telecommunications optical fibre. To ensure light at 895 nm propagates in the fundamental mode 5 µm core diameter optic fibre is spliced onto the ends of the standard telecom fibre. Static polarisation controllers (SPC) compensate for polarisation evolution in the fibre and return the light into its input polarisation state to ensure either reflection or transmission at the polarisation beam splitters (PBS). The photons are detected using silicon single-photon avalanche photodiodes (Si-SPAD).

The light is then incident on a 50:50 fibre coupled beam splitter in Bob which randomly routes the photon to one of two polarisation beam splitters (PBS) which are used to make measurements of the polarisation state of the photon in either the linear or circular polarisation basis set. These PBS cubes separate the S polarisation (electric field perpendicular to plane of incidence) and P polarisation (electric field parallel to plane of incidence) components by reflecting the S component at the dielectric beamsplitter coating, while allowing the P component to pass [64], [65]. A static polarisation controller (SPC) then directs the photons onto either the designated detector for measuring a binary 0 or binary 1 value via the PBS in each basis set. This is achieved by the controlled bending of the fibre which introduces birefringence [66]. The change in the refractive induced by bending is given by the following expression

$$\delta n = -0.136 \times \left(\frac{r}{R} \right)^2 \qquad \text{Equation (3.10)}$$

where r is the radius of the fibre and R is the bend radius [67]. Before any key is transmitted, Alice sends an alignment optical pulse to Bob which ensures that the polarisation axes between the two parties are correctly aligned. Unambiguous discrimination is only achieved when Alice encodes and Bob measures in the same polarisation basis set. Imperfections in Bob's optical components resulted in a loss of 4.76 dB in his measurement apparatus.

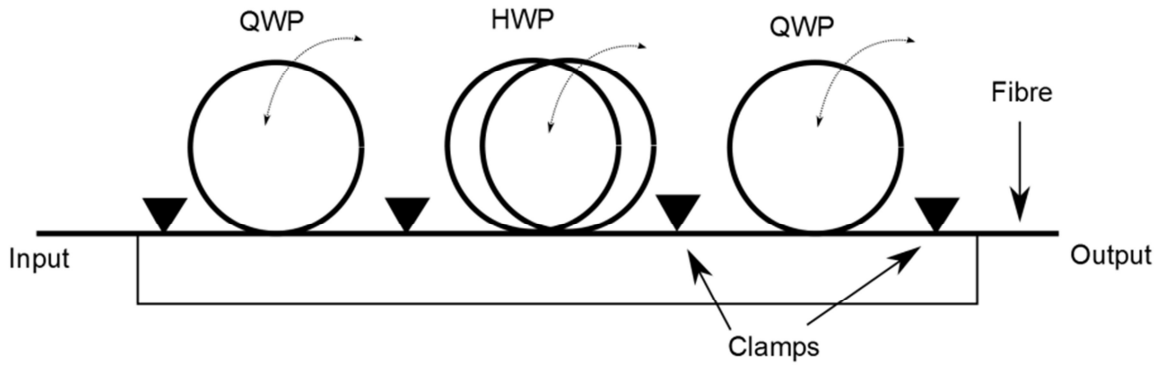

Figure 3.26. Schematic of the in-line fibre optic polarisation controller. Using Equation (3.10) it can be shown that the induced phase change due to bending is given by $\Delta\phi = 0.136 \times N \times 8\pi r^2 / \lambda R$*, where N is the number of loops. If the bend radius is given by* $R = 0.136 \times 8\pi r^2 / \lambda R$ *then 1 loop creates a quarter waveplate (QWP) and two loops creates a half wave plate (HWP) [68].*

3.6.2 Data acquisition and analysis

The electrical signal of one of the SPADs was used as the constant fraction discriminator (CFD) of the Becker and Hickl SPC-600 TCSPC card. Due to the poor resolution of the macro clock in the SPC-600 when running in FIFO mode, which is discussed in more detail in Chapter 2, the card was run in Histogram mode to avoid issues which resulted in the arrival time of the input electrical pulses being rounded up or down to the nearest multiple of 50 ns. This has the disadvantage that the timing information of an individual time tag is lost. Figure 3.27 shows a typical histogram

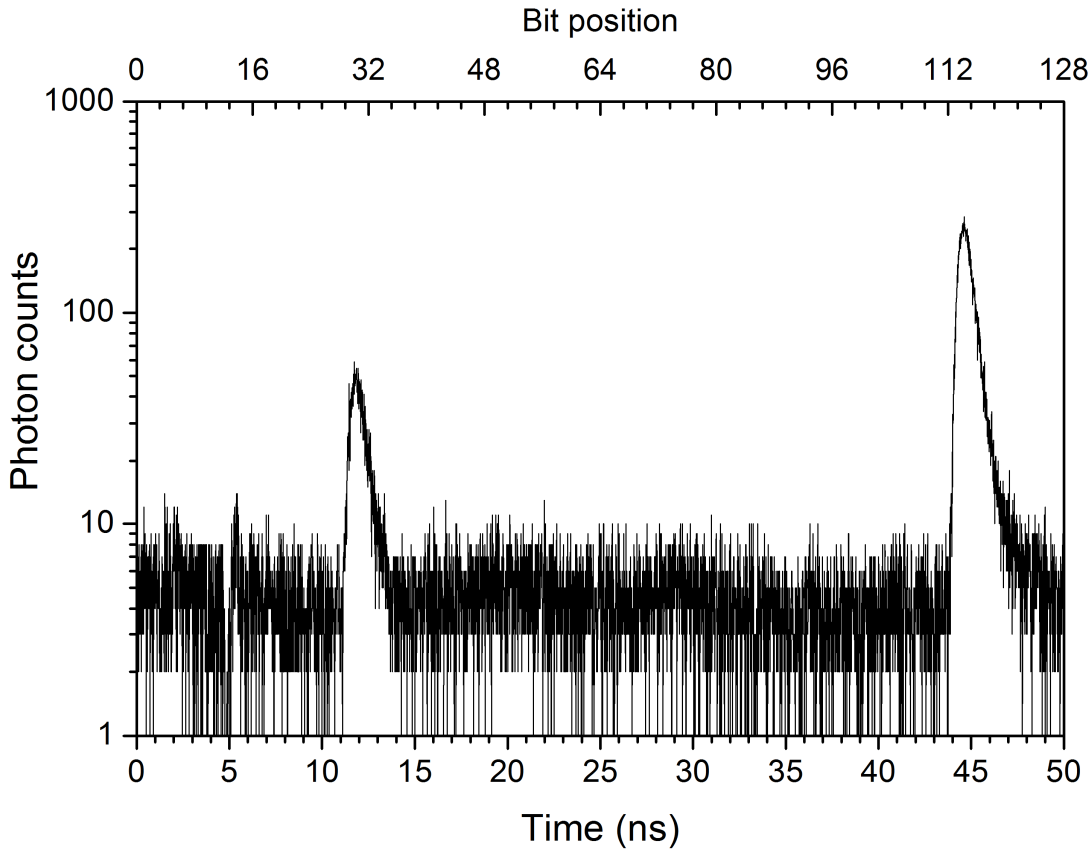

Figure 3.27. A typical histogram produced from the system for one detector designated for measuring vertically polarised photons. A horizontal polarisation state is produced at 11.7 ns (bit 30) and a vertical polarisation state is observed at 44.5 ns (bit 114). The horizontal polarisation is visible due to the PER set to a deliberate poor value for illustrative purposes. The time axis represents two periods (50 ns) of the system clock frequency (25ns) and shows two unequally temporally spaced laser pulses. The pulse pattern generator outputted a 128 bit pattern (top x-axis) with bits 30 and 114 active to trigger the excitation laser at 784 nm.

produced from the electrical signal from a single detector. In this example the detector is designated for recording photons encoded with a vertical polarisation. The issue of a non-periodic laser pulse discussed in section 3.6.1 can clearly be seen. The time scale represents two periods of the system clock containing two pulses, giving a mean pulse train of 40 MHz. The photons encoded with a vertical polarisation are seen at 5.85 ns (bit 30) and the photons encoded with a horizontal polarisation are seen at 22.26 ns (bit 114). The ratio of the heights of the peaks at the two locations is determined by the polarisation extinction ratio (ER) of the beam splitter in Bob and was measured to be 545:1 (Figure 3.27 shows an ER of about 4.7:1 for clarity). The higher the extinction ratio the lower the resulting quantum bit error rate (QBER) value will be. To reduce the effects of dark counts on the QBER, a 300 ps gate is opened on the peaks at the expected locations of the bit times. In Figure 3.27 the QBER may be calculated by dividing the total counts in a 300 ps window centered on bit 114 (incorrect counts) by the total count contained in a 300 ps window centred on 30 and 114. This also enables the sifted bit rate to be calculated which is used to determine the overall net bit rate in section 3.6.3. The above technique only uses one detector. For a complete analysis a similar procedure is completed for the three remaining detectors. Had TCSPC modules like the GuideTech GT65X time interval analyser, which is used in Chapter 4 or the HydraHarp 400, which is used in Chapter 5, been available at the time of the experiment this would have allowed the simultaneous recording of photon events on the four detectors.

3.6.3 Experimental Results

The quantum bit error rate was measured at a range of different excitation powers. Figure 3.28 shows the variation in the QBER against excitation power for 0 km and 2 km transmission distances. 0 and 2 km transmission distance were chosen due to the availability of fibre reels and also the relatively low photon flux which would have resulted at distances greater than 2 km. At higher excitation powers, which results in a higher photon flux the QBER decreases. The lowest QBER measured was 1.22% at 0 km and 6.21% at 2 km. At the lowest $g^{(2)}(0)$ of 0.32, which is produced by an excitation power of 0.25 µW, the QBER for 0 km was 21.9%. The fraction of bits which must be discarded for error correction is given by Cascade error correction protocol [69]:

$$R_{net} = \left[1 - f_p H_2\left(QBER\right)\right] R_{sifted} \qquad \text{Equation (3.11)}$$

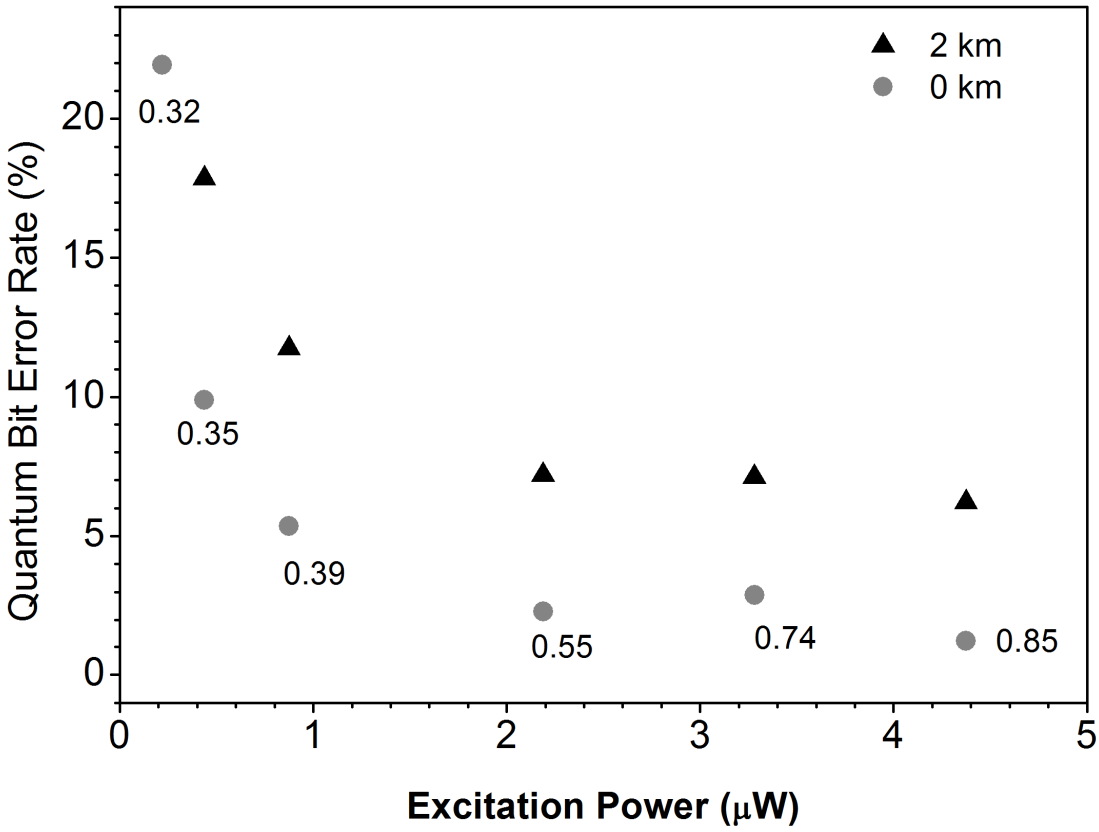

Figure 3.28. The QBER against the excitation power at the sample surface using the quantum dot microcavity single photon source. The black triangles denote a transmission distance of 2 km while the grey circles denote a transmission distance of 0 km. The numerical value next to each data point is the value of the autocorrelation function $g^{(2)}(0)$ *for that excitation power.*

where R_{net} is the net bit rate, R_{sifted} is the sifted bit rate after temporal filtering, f_p is a measure of the additional inefficiency of the error correction protocol when compared to the theoretical Shannon limit and $H_2(QBER)$ is the binary entropy function and is given by

$$H_2(QBER) = -QBER\log_2(QBER) - (1-QBER)\log_2(1-QBER) \qquad \text{Equation (3.12)}$$

When using the Cascade error correction protocol [69] $f_p = 1.16$. Cascade error correction was the preferred choice over other protocols like Winnow and low density parity check (LDPC) as it is the most efficient at correcting errors up to about 11% [70].

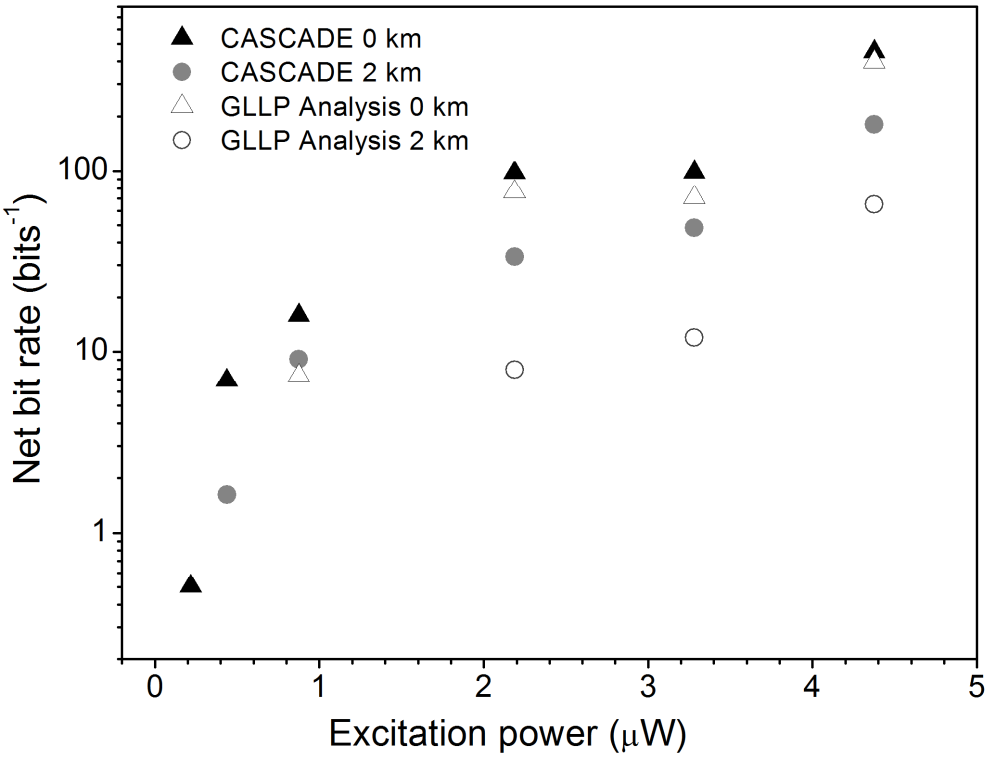

Figure 3.29. The net bit rates shown against the excitation power on the sample surface using the quantum dot microcavity single photon source. The black solid triangles denote a transmission distance of 0 km while the grey solid circles denote a transmission distance of 2 km. The unfilled points denote the bit rates obtained using the GLLP analysis described in the text.

The filled points in Figure 3.29 shows the calculated net bit rate as a function of the excitation power for 0 and 2 km transmission distances when only considering the Cascade error correction protocol. This analysis does not take into consideration the extra additional bits which must be discarded as a result of the photon number splitting attack (PNS) [71]. Work developed by Gottesman, Lo, Lükenhaus and Preskill (GLLP) leads to a more complete security analysis based on imperfect devices and can be used to calculate the secure bit rate. In this proof the bit rate is given by the following

$$R_{net} = \left[(1-\Delta) - f_p H_2(Q) - (1-\Delta) f_p H_2\left(\frac{Q}{1-\Delta}\right) \right] R_{sifted} \qquad \text{Equation (3.13)}$$

where Δ is the fraction of the bits transmitted by Alice which are intercepted by Eve. To establish a lower bound on the secure key rate it is assumed that Eve intercepts every multiphoton pulse emitted by Alice so that $\Delta \approx g^{(2)}(0)\mu^2/2$ [72]. The unfilled data points in Figure 3.29 represent the bit rate obtained when Equation (3.13) is applied. Figure 3.30 shows the secure bit rate per pulse for various simulated single photon

emitters with varying $g^{(2)}(0)$ values and also for a weak coherent pulse (WCP) which considers the PNS attack.

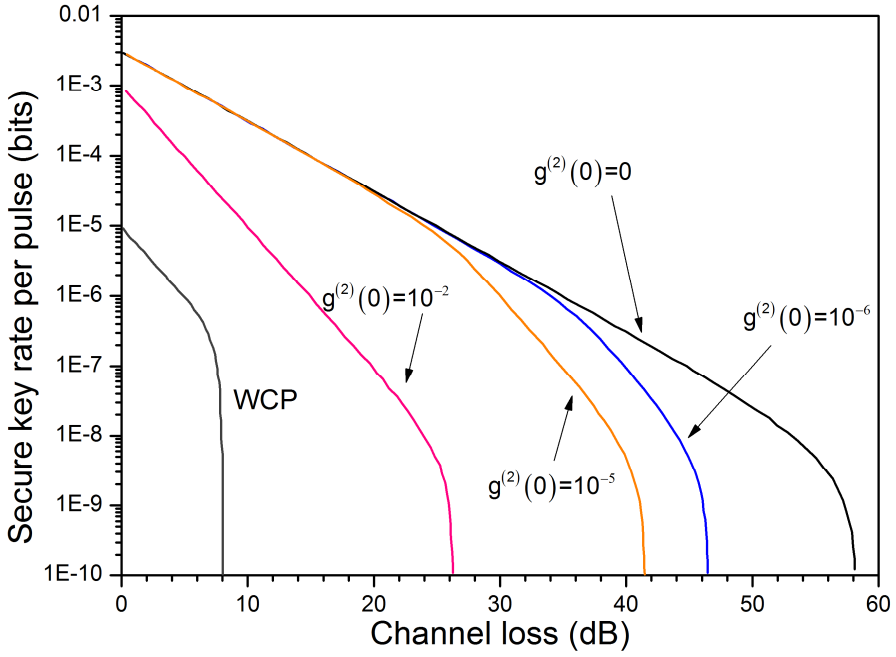

Figure 3.30. Secure key rate as a function of channel loss for various simulated single photon emitters with different $g^{(2)}(0)$ values and a weak coherent pulse (WCP [73]).The analysis is based on 100% efficient detectors.

The bit rate for the WCP decreases much faster than an ideal single-photon source (SPS) as the SPS does not suffer from the PNS attack. The rate at which the bit rate decreases is only proportional to the channel loss for an ideal SPS. For the WCP as the channel loss is increased the effect of multi-photon pulses increases which forces us to reduce the mean photon number per pulse. For a SPS with intermediate values $0 \le g^{(2)}(0) \le 1$ they behave like an ideal SPC at short distances where the bit rate decreases with transmission distance but at longer distances the effect of multi-photon pulses increases and they behave similarly to that of a WCP [53]. This demonstrates that although there is a definite gain to be obtained by using single-photon pulses, for their true potential to be realised values of $g^{(2)}(0)$ need to be significantly improved. Practically this means that using the lowest reported value of $g^{(2)}(0)$ of ~0.05, means that compared to an ideal SPS the maximum channel loss is reduced by ~30 dB [74].

3.7 Discussion and Conclusions

This chapter has looked at the issue of generating single photons which exhibit sub-Poissonian statistics using a quantum dot embedded in a micropillar cavity with an emission wavelength of 984.5 nm. The quantum dot source was used in a test bed

implementation of the BB84 protocol for QKD. Autocorrelation measurements were performed to characterise how closely the quantum dot behaves like a true single-photon emitter at a series of different excitation powers. The lowest measured $g^{(2)}(0)$ value was 0.32 at an excitation power of 0.25 μW rising to 085 at the highest excitation power of 5 μW. The highest photon emission rate from the quantum dot sample was 4 MHz which was calculated assuming an 11% coupling efficiency of the microscope into 9 μm diameter core fibre and a detector efficiency of 38% at a wavelength of 895 nm.

Due to difficulties with the polarisation modulator only three of the four states required for the BB84 protocol could be generated. The modulator was also a resonant device which meant that the only clock rate at which the system could be operated at was 40 MHz. The maximum observed value for the primary excited state lifetime was 563 ps which would limit the maximum excitation pulse repetition rate to several hundred megahertz. This would allow a much higher photon flux. In addition if the free space modulator could be replaced by an in-line fibre coupled version the loss of the system could be significantly reduced.

As a result of the non-equally spaced bit locations for the four polarisation states as seen in Figure 3.24 it was necessary to pulse the laser non-periodically to ensure that the optical pulse when inside the polarisation crystal was synchronised with the electrical signal for each of the polarisation states. This leaves the system vulnerable to a potential eavesdropper who can measure the temporal separation between pulses to gain information on the state sent by Alice. In a more realistic scenario the laser pulse repetition frequency should be kept constant.

A series of measurements investigating how the QBER and the net bit rate varied as the excitation power was varied is shown in Figure 3.28 and Figure 3.29 for a transmission distance of 0 km and 2 km. The net bit rate was calculated using both the Cascade error correction protocol and the GLLP security analysis. The highest bit rate obtainable using the GLLP analysis was 65 bits/sec for 2km and 396 bits/sec for 0 km. The net bit rate obtained using Cascade error correction is higher as it does not take into account those extra bits which must be sacrificed because of the PNS. The highest bit rate obtainable using Cascade error correction was 179 bits/sec for 2km and 453 bits/sec for 0 km. Other research groups have used single-photon sources in a QKD system. The Toshiba research group used an InAs quantum dot operating at ~1.3 μm over 35 km of

optical fibre using phase encoding with a Mach Zehnder interferometer [72]. They reported a $g^{(2)}(0)$ value of 0.16 and a secure bit rate of ~2 bits/sec at 35 km using GLLP analysis. The reported single-photon efficiency was 4.6% at a clock rate of 1 MHz. In 2010 researchers in Japan reported the lowest $g^{(2)}(0)$ value of 0.055 obtained at a wavelength of 1.5 μm using a quantum dot structure [75]. The single photon efficiency was 5.8% corresponding to a single photon per pulse of 1.2 MHz. Using simulations based on Waks *et al.* [53] a single photon source with a $g^{(2)}(0)$ of 0.055 can distribute secure keys over 6 dB more channel loss compared to a SPS with a $g^{(2)}(0)$ value of 0.85. One of the highest reported emission rate for a quantum dot microcavity was made by Strauf *et al.* with a emission rate of 31 MHz after correction for detection efficiency, displaying a $g^{(2)}(0)$ value of 0.4 [59]. If this single-photon source could be integration into the QKD system described here, which has an emission rate of ~7.75 times the source used in this chapter then a calculated secure bit rate of 1653 bits/sec could be expected using a $g^{(2)}(0)$ of 0.4.

The issue of source efficiency and collection efficiency for a single-photon source was examined by Gérard *et al* in 2010 [76]. They used self-assembled InAs quantum dots embedded in a GaAs Photonic nanowire which was carefully tapered at one end and with a metal-dielectric mirror at the other. Using a 0.7 NA collection lens they obtained a source efficiency, defined by the probability of collecting a photon into the first lens in the system, of 0.72 (72%). This corresponded to a single-photon emission rate into the first lens of 55 MHz when optically pumped at saturation using a Ti:sapphire laser at a repetition rate of 76 MHz. The emission wavelength of the source was 915.2 nm which was maintained at 5 K. A $g^{(2)}(0)$ value of less than 0.008 was obtained. They stated that photonic nanowires have an advantage over quantum dot cavity single-photon emitters as cavities which are detuned from the QD can contribute to the cavity mode via coupling to the continuum of states leading to multiphoton pulses under non-resonant excitation, thereby increasing the $g^{(2)}(0)$ value. The addition of a source similar to the one developed developed by Gérard *et al.*, which is at least an order of magnitude more efficient than the source presented in this chapter, into the QKD system here would be a huge benefit to the bit rate which could be obtained from the system.

The necessity for operating the QKD system described in this chapter with liquid helium places restrictions on the practicality of such a system. Already demonstrations of single-photon emission at room temperature has been demonstrated in molecules

[77], colour centres in diamonds [78] and nanocrystals [79]. Philip Grangier's group in Paris, used the nitrogen-vacancy colour centre in a diamond nonocrystal in a free-space QKD system employing polarisation encoding at 1.55 μm. They obtained a $g^{(2)}(0)$ value of 0.15 and a bit rate of 1.67 kbits/sec at 30.5 metres [80].

Recently the interest in using quantum dots in a QKD system has dropped due to the development of decoys states which can deliver superior bits rates with lasers offering a much simpler solution [81]. In 2008 Dixon *et al.* demonstrated a gigahertz clocked decoy-protocol quantum key distribution system [82]. A secure bit rate of 1.02 Mbits/s was obtained over a fibre distance of 20 km while 10.1 kbit/s was achieved for 100km. By simply sending decoy pulses, Alice and Bob are able to prevent the photon number splitting attack. However interest in single-photon sources could be reinvigorated for applications in distributing entangled states over long distances using quantum repeaters which require single-photon sources [83].

3.8 Acknowledgments

The author would like to thank Dr Robert Collins for his help with the experiments carried out in this chapter. Additionally the author would like to thank Dr Karen Gordon for designing the original microscope and cooling system for the characterisation of the quantum dots, Dr Aongus McCarthy for his help in the optical alignment of the system and Mr Peter Heron who designed and manufactured the optical component holders for the microscope. The author would like to thank Professor Mark Hopkinson for the growth of the quantum dot samples used in this chapter and to Dr Jane Timpson, Dr Ruth Oulton, Dr Maxim Makhonin, Professor Maurice Skolnick and Professor Mark Fox who did some initial characterisations of the samples.

References

[1] D. Bouwmeester, J. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "*Experimental quantum teleportation"*. Nature, 1997. **390**(6660): p. 575-579.

[2] E. Knill, R. Laflamme, and G.J. Milburn, "*A scheme for efficient quantum computation with linear optics"*. Nature, 2001. **409**(6816): p. 46-52.

[3] P. Townsend, "*Secure key distribution system based on quantum cryptography"*. Electronics Letters, 1994. **30**(10): p. 809-811.

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "*Quantum cryptography"*. Reviews of Modern Physics, 2002. **74**(1): p. 145-195.

[5] D. Bimberg, E. Stock, A. Lochmann, A. Schliwa, J.A. Tofflinger, W. Unrau, M. Munnix, S. Rodt, V.A. Haisler, A.I. Toropov, A. Bakarov, and A.K. Kalagin, "*Quantum Dots for Single- and Entangled-Photon Emitters"*. Photonics Journal, IEEE, 2009. **1**(1): p. 58-68.

[6] M. Henini, "*Handbook of self assembled semiconductor nanostructures for novel devices in photonics and electronics"* 2008: Elsevier Science.

[7] P. Michler, "*Single semiconductor quantum dots"* 2009: Springer Verlag.

[8] A. Kuther, M. Bayer, A. Forchel, A. Gorbunov, V. Timofeev, F. Schafer, and J. Reithmaier, "*Zeeman splitting of excitons and biexcitons in single In 0.60 Ga 0.40 As/GaAs self-assembled quantum dots"*. Phys. Rev. B, 1998. **58**(7508): p. 158.

[9] S. Buckley, K. Rivoire, and J. Vučković, "*Engineered quantum dot single-photon sources"*. Reports on Progress in Physics, 2012. **75**(12): p. 126503.

[10] Z. Yuan, B.E. Kardynal, R.M. Stevenson, A.J. Shields, C.J. Lobo, K. Cooper, N.S. Beattie, D.A. Ritchie, and M. Pepper, "*Electrically Driven Single-Photon Source"*. Science, 2002. **295**(5552): p. 102-105.

[11] J. Kim, O. Benson, H. Kan, and Y. Yamamoto, "*A single-photon turnstile device"*. Nature, 1999. **397**(6719): p. 500-503.

[12] C. Santori, D. Fattal, J. Vuckovic, G. Solomon, and Y. Yamamoto, "*Single-photon generation with InAs quantum dots"*. New Journal of Physics, 2004. **6**(1): p. 89.

[13] B. Alloing, C. Zinoni, V. Zwiller, L.H. Li, C. Monat, M. Gobet, G. Buchs, A. Fiore, E. Pelucchi, and E. Kapon, "*Growth and characterization of single quantum dots emitting at 1300 nm"*. Applied Physics Letters, 2005. **86**(10): p. 101908-3.

[14] J. Tatebayashi, M. Nishioka, and Y. Arakawa, "*Over 1.5 μm light emission from InAs quantum dots embedded in InGaAs strain-reducing layer grown by metalorganic chemical vapor deposition"*. Applied Physics Letters, 2001. **78**(22): p. 3469-3471.

[15] M. Pelton, J. Vuckovic, G. Solomon, C. Santori, B. Zhang, J. Plant, and Y. Yamamoto, "*An efficient source of single photons: a single quantum dot in a micropost microcavity"*. Physica E: Low-dimensional Systems and Nanostructures, 2002. **89**(23): p. 564-567.

[16] B. Zhang, G.S. Solomon, M. Pelton, J. Plant, C. Santori, J. Vuckovic, and Y. Yamamoto, "*Fabrication of InAs quantum dots in AlAs/GaAs DBR pillar microcavities for single photon sources"*. Journal of Applied Physics, 2005. **97**(7): p. 073507.

[17] C. Sheppard, "*Approximate calculation of the reflection coefficient from a stratified medium"*. Pure and Applied Optics: Journal of the European Optical Society Part A, 1995. **4**: p. 665.

[18] G.S. Buller and R.J. Collins, "*Single-photon generation and detection"*. Measurement Science and Technology, 2010. **21**: p. 012002.

[19] E.M. Purcell, H.C. Torrey, and R.V. Pound, "*Resonance Absorption by Nuclear Magnetic Moments in a Solid"*. Physical Review, 1946. **69**(1-2): p. 37-38.

[20] M. Fox, "*Quantum optics: an introduction"* 2006: Oxford University Press.

[21] J.M. Gérard, B. Sermage, B. Gayral, B. Legrand, E. Costard, and V. Thierry-Mieg, "*Enhanced Spontaneous Emission by Quantum Boxes in a Monolithic Optical Microcavity"*. Physical Review Letters, 1998. **81**(5): p. 1110-1113.

[22] A. Badolato, K. Hennessy, M. Atatüre, J. Dreiser, E. Hu, P.M. Petroff, and A. Imamoğlu, "*Deterministic coupling of single quantum dots to single nanocavity modes"*. Science, 2005. **308**(5725): p. 1158-1161.

[23] L.K. Ivan N. Stranski, "*Abhandlungen der Mathematisch-Naturwissenschaftlichen Klasse IIb"*. Akademie der Wissenschaften Wien, 1938. **146**: p. 797-810.

[24] H. Kissel, U. Müller, C. Walther, W.T. Masselink, Y.I. Mazur, G.G. Tarasov, and M.P. Lisitsa, "*Size distribution in self-assembled InAs quantum dots on GaAs (001) for intermediate InAs coverage"*. Physical Review B, 2000. **62**(11): p. 7213-7218.

[25] K. Barnham and D. Vvedensky, "*Low-dimensional semiconductor structures: fundamentals and device applications"* 2008: Cambridge Univ Pr.

[26] S. Reitzenstein and A. Forchel, "*Quantum dot micropillars"*. Journal of Physics D: Applied Physics, 2010. **43**(3): p. 033001.

[27] R. Collins, P. Clarke, V. Fernandez, K. Gordon, M. Makhonin, J. Timpson, A. Tahraoui, M. Hopkinson, A. Fox, and M. Skolnick, "*Quantum key distribution system in standard telecommunications fiber using a short wavelength single photon source"*. Journal of Applied Physics, 2010. **107**(7): p. 073102-073102-6.

[28] *"SPCM-AQR single photon counting module Perkin Elmer datasheet", 2005, http://www.htds.fr/doc/optronique/militaireAerospace/SPCM-AQR.pdf, date accessed:02/10/2012*

[29] P.H. Lissberger and W.L. Wilcock, "*Properties of All-Dielectric Interference Filters. II. Filters in Parallel Beams of Light Incident Obliquely and in Convergent Beams"*. Journal of the Optical Society of America, 1959. **49**(2): p. 126-128.

[30] X. Baillard, A. Gauguet, S. Bize, P. Lemonde, P. Laurent, A. Clairon, and P. Rosenbusch, "*Interference-filter-stabilized external-cavity diode lasers"*. Optics Communications, 2006. **266**(2): p. 609-613.

[31] J. Vuckovic, C. Santori, D. Fattal, M. Pelton, G.S. Solomon, Z. Bingyang, J. Plant, and Y. Yamamoto. "*Single photons and entangled photons from a quantum dot"*. in *Electron Devices Meeting, 2002. IEDM '02. International*. 2002.

[32] *"Compact multi dimensional translation stages", Piezosystem Jena,http://www.piezosystem.com/uploads/media/dl_mg_1227623716_01.pdf, date accessed:26/9/2012*

[33] J.M. Bennett and E.J. Ashley, "*Infrared Reflectance and Emittance of Silver and Gold Evaporated in Ultrahigh Vacuum"*. Applied Optics, 1965. **4**(2): p. 221-224.

[34] "*Instruction manual for continous flow cryostat CF 1104*", E.O.O.T. Oxford Instruments Limited,1988

[35] S. Rudin, T.L. Reinecke, and M. Bayer, "*Temperature dependence of optical linewidth in single InAs quantum dots"*. Physical Review B, 2006. **74**(16): p. 161305.

[36] J.P. Reithmaier, G. Sek, A. Loffler, C. Hofmann, S. Kuhn, S. Reitzenstein, L.V. Keldysh, V.D. Kulakovskii, T.L. Reinecke, and A. Forchel, "*Strong coupling in a single quantum dot-semiconductor microcavity system"*. Nature, 2004. **432**(7014): p. 197-200.

[37] B. Tell, K. Brown‐Goebeler, R. Leibenguth, F. Baez, and Y. Lee, "*Temperature dependence of GaAs‐AlGaAs vertical cavity surface emitting lasers"*. Applied Physics Letters, 1992. **60**(6): p. 683-685.

[38] A. Laucht, F. Hofbauer, N. Hauke, J. Angele, S. Stobbe, M. Kaniber, G. Böhm, P. Lodahl, M.C. Amann, and J.J. Finley, "*Electrical control of spontaneous emission and strong coupling for a single quantum dot"*. New Journal of Physics, 2009. **11**(2): p. 023034.

[39] A. Högele, S. Seidl, M. Kroner, K. Karrai, R.J. Warburton, B.D. Gerardot, and P.M. Petroff, "*Voltage-controlled optics of a quantum dot"*. Physical Review Letters, 2004. **93**(21): p. 217401.

[40] W.G. Fastie, H. Crosswhite, and P. Gloersen, "*Vacuum Ebert grating spectrometer"*. Journal of the Optical Society of America, 1958. **48**(2): p. 106-109.

[41] J.P.E. David, J.B. Anthony, J.D. Samuel, A.N. Christine, A.R. David, and J.S. Andrew, "*Cavity-enhanced radiative emission rate in a single-photon-emitting diode operating at 0.5 GHz"*. New Journal of Physics, 2008. **10**(4): p. 043035.

[42] J. Timpson, D. Sanvitto, A. Daraei, P. Guimaraes, H. Vinck, S. Lam, D. Whittaker, M. Skolnick, A. Fox, and C. Hu, "*Single photon sources based upon single quantum dots in semiconductor microcavity pillars"*. Journal of Modern Optics, 2007. **54**(2-3): p. 453-465.

[43] P. Borri, W. Langbein, S. Schneider, U. Woggon, R.L. Sellin, D. Ouyang, and D. Bimberg, "*Ultralong dephasing time in InGaAs quantum dots"*. Physical Review Letters, 2001. **87**(15): p. 157401.

[44] L. Besombes, K. Kheng, L. Marsal, and H. Mariette, "*Acoustic phonon broadening mechanism in single quantum dot emission"*. Physical Review B, 2001. **63**(15): p. 155307.

[45] D. Gammon, E. Snow, B. Shanabrook, D. Katzer, and D. Park, "*Homogeneous linewidths in the optical spectrum of a single gallium arsenide quantum dot"*. Science, 1996. **273**(5271): p. 87-90.

[46] T. Yoshie, A. Scherer, H. Chen, D. Huffaker, and D. Deppe, "*Optical characterization of two-dimensional photonic crystal cavities with indium arsenide quantum dot emitters"*. Applied Physics Letters, 2001. **79**(1): p. 114-116.

[47] R. Thompson, R. Stevenson, A. Shields, I. Farrer, C. Lobo, D. Ritchie, M. Leadbeater, and M. Pepper, "*Single-photon emission from exciton complexes in individual quantum dots*". Physical Review B, 2001. **64**(20): p. 201302.

[48] C. Santori, D. Fattal, J. Vučković, G.S. Solomon, E. Waks, and Y. Yamamoto, "*Submicrosecond correlations in photoluminescence from InAs quantum dots*". Physical Review B, 2004. **69**(20): p. 205324.

[49] R.H. Hadfield, M.J. Stevens, S.S. Gruber, A.J. Miller, R.E. Schwall, R.P. Mirin, and S.W. Nam, "*Single photon source characterization with a superconducting single photon detector*". Optics Express, 2005. **13**(26): p. 10846-10853.

[50] K. Hennessy, A. Badolato, M. Winger, D. Gerace, M. Atatüre, S. Gulde, S. Fält, and A.I. EL Hu, "*Quantum nature of a strongly coupled single quantum dot–cavity system*". Nature, 2007. **445**(7130): p. 896-899.

[51] D. Press, S. Götzinger, S. Reitzenstein, C. Hofmann, A. Löffler, M. Kamp, A. Forchel, and Y. Yamamoto, "*Photon Antibunching from a Single Quantum-Dot-Microcavity System in the Strong Coupling Regime*". Physical Review Letters, 2007. **98**(11): p. 117402.

[52] I. Robert, E. Moreau, J. Gérard, and I. Abram, "*Towards a single-mode single photon source based on single quantum dots*". Journal of luminescence, 2001. **94**: p. 797-803.

[53] E. Waks, C. Santori, and Y. Yamamoto, "*Security aspects of quantum key distribution with sub-Poisson light*". Physical Review A, 2002. **66**(4): p. 042315.

[54] R. Brouri, A. Beveratos, J.P. Poizat, and P. Grangier, "*Photon antibunching in the fluorescence of individual color centers in diamond*". Optics Letters, 2000. **25**(17): p. 1294-1296.

[55] B.R. Masters, "*Confocal microscopy and multiphoton excitation microscopy: the genesis of live cell imaging*". Vol. 72. 2006: Society of Photo Optical.

[56] *"Analytical T900 Software V6.0", Edinburgh Instruments Ltd,date*

[57] D.V. O'connor and D. Phillips, "*Time-correlated single photon counting*". Vol. 102. 1984: Academic Press London.

[58] O. Labeau, P. Tamarat, and B. Lounis, "*Temperature dependence of the luminescence lifetime of single CdSe/ZnS quantum dots*". Physical review letters, 2003. **90**(25): p. 257404.

[59] S. Strauf, N.G. Stoltz, M.T. Rakher, L.A. Coldren, P.M. Petroff, and D. Bouwmeester, "*High-frequency single-photon source with polarization control*". Nature Photonics, 2007. **1**(12): p. 704-708.

[60] E. Moreau, I. Robert, L. Manin, V. Thierry-Mieg, J. Gérard, and I. Abram, "*A single-mode solid-state source of single photons based on isolated quantum dots in a micropillar*". Physica E: Low-dimensional Systems and Nanostructures, 2002. **13**(2): p. 418-422.

[61] J. Wilson and J.F.B. Hawkes, "*Optoelectronics-an introduction*". 1989.

[62] *"EO modulator driver and source. Models 3363-A, 3363-B and 3363-C", 2003, http://assets.newport.com/webDocuments-EN/images/15198.PDF, date accessed:16/5/2012*

[63] P. Townsend, "*Experimental investigation of the performance limits for first telecommunications-window quantum cryptography systems*". IEEE Photonics Technology Letters, 1998. **10**(7): p. 1048-1050.

[64] "*Beam splitter and combiners*", Oz Optics, Ottawa, Canada

[65] L. Li and J.A. Dobrowolski, "*High-Performance Thin-Film Polarizing Beam Splitter Operating at Angles Greater than the Critical Angle*". Applied Optics, 2000. **39**(16): p. 2754-2771.

[66] R. Ulrich, S. Rashleigh, and W. Eickhoff, "*Bending-induced birefringence in single-mode fibers*". Optics Letters, 1980. **5**(6): p. 273-275.

[67] H. Lefevre, "*Single-mode fibre fractional wave devices and polarisation controllers*". Electronics Letters, 1980. **16**(20): p. 778-780.

[68] A. Kumar and A.K. Ghatak, "*Polarization of light with applications in optical fibers*" 2011: SPIE Press.

[69] G. Brassard and L. Salvail, "*Secret Key Reconciliation by public discussion*". Lecture Notes in Computer Science, 1994. **765**: p. 0410.

[70] G. Van Assche, "*Quantum cryptography and secret-key distillation*" 2006: Cambridge University Press.

[71] N. Lütkenhaus and M. Jahma, "*Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack*". New Journal of Physics, 2002. **4**: p. 44.

[72] P. Intallura, M. Ward, O. Karimov, Z. Yuan, P. See, P. Atkinson, D. Ritchie, and A. Shields, "*Quantum communication using single photons from a semiconductor quantum dot emitting at a telecommunication wavelength*". Journal of Optics A: Pure and Applied Optics, 2009. **11**: p. 054005.

[73] H. Takesue, S. Nam, Q. Zhang, R. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "*Quantum key distribution over a 40-dB channel loss using*

superconducting single-photon detectors". Nature Photonics, 2007. **1**(6): p. 343-348.

[74] C. Santori, D. Fattal, J. Vuckovic, G.S. Solomon, and Y. Yamamoto, "*Indistinguishable photons from a single-photon device".* Nature, 2002. **419**(6907): p. 594-597.

[75] K. Takemoto, Y. Nambu, T. Miyazawa, K. Wakui, S. Hirose, T. Usuki, M. Takatsu, N. Yokoyama, K. Yoshino, and A. Tomita, "*Transmission Experiment of Quantum Keys over 50 km Using High-Performance Quantum-Dot Single-Photon Source at 1.5 mum Wavelength".* Applied Physics Express, 2010. **3**(9): p. 2802.

[76] J. Claudon, J. Bleuse, N.S. Malik, M. Bazin, P. Jaffrennou, N. Gregersen, C. Sauvan, P. Lalanne, and J.-M. Gerard, "*A highly efficient single-photon source based on a quantum dot in a photonic nanowire".* Nature Photonics, 2010. **4**(3): p. 174-177.

[77] B. Lounis and W.E. Moerner, "*Single photons on demand from a single molecule at room temperature".* Nature, 2000. **407**(6803): p. 491-493.

[78] T.M. Babinec, J.M. HausmannBirgit, M. Khan, Y. Zhang, J.R. Maze, P.R. Hemmer, and M. Loncar, "*A diamond nanowire single-photon source".* Nature Nanotechnology, 2010. **5**(3): p. 195-199.

[79] P. Michler, A. Imamoglu, M.D. Mason, P.J. Carson, G.F. Strouse, and S.K. Buratto, "*Quantum correlation among photons from a single quantum dot at room temperature".* Nature, 2000. **406**(6799): p. 968-970.

[80] R. Alleaume, F. Treussart, G. Messin, Y. Dumeige, J. Roch, A. Beveratos, R. Brouri-Tualle, J. Poizat, and P. Grangier, "*Experimental open-air quantum key distribution with a single-photon source".* New Journal of Physics, 2004. **6**(1): p. 92.

[81] H.-K. Lo, X. Ma, and K. Chen, "*Decoy State Quantum Key Distribution".* Physical Review Letters, 2005. **94**(23): p. 230504.

[82] A. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, "*Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate".* Optics Express, 2008. **16**: p. 18790.

[83] N. Sangouard, C. Simon, J. Minář, H. Zbinden, H. de Riedmatten, and N. Gisin, "*Long-distance entanglement distribution with single-photon sources".* Physical Review A, 2007. **76**(5): p. 050301.

Chapter 4

Robust GHz clocked fibre quantum key distribution

4.1 Introduction

Previous chapters have introduced the concept of quantum key distribution (QKD) and gave an overview of the electro-optics components required in many modern QKD systems. This chapter will outline a novel method for eliminating the random polarisation evolution of light travelling in standard telecoms fibre which is integrated into a QKD system. If this effect were to remain it would cause massive encoding errors in a fibre based system. In addition, unlike existing QKD systems which use active optical components to make a basis set selection which can cause thermal instability in fibre systems, the one implemented in this chapter uses passive optical components. Most QKD systems in use today operate at a wavelength in the third telecommunications window around 1550 nm benefiting from the low fibre attenuation of 0.2 dB/km of standard telecommunications fibre used in the global communication infrastructure [1]. The system described in this chapter operates at a wavelength of 850 nm and although it suffers from a higher fiber attenuation of 2.2 dB/km it can make use of the mature silicon single-photon detector technologies which offer superior timing jitter, detection efficiency and dark count rate characteristics than the alternatives at 1550 nm. Operating at a wavelength of 850 nm also avoids the spectrally wide spontaneous Raman scattering background generated by high power classical data channels which can considerably increase the quantum bit error rate (QBER) in QKD systems [2]. The QKD system described in this chapter is operated using a variety of single-photon avalanche photodiode (SPAD) detectors including thick and thin junction SPADs as well as a superconducting nanowire device resulting in the most comprehensive comparison of different detector technologies in a QKD environment. This comparison of detectors in addition to theoretically modeling how the detector affects the performance of a QKD system could assist engineers in designing detectors which are optimised for use in quantum key distribution systems in the future.

4.1.1 Operation of the QKD system

The experimental system is shown in Figure 4.2. The setup is based on an asymmetric double Mach-Zehnder design using 5 µm core diameter panda eye polarisation maintaining fibre to maximise interferometric fringe visibility. The fibre

beamsplitters/combiners used are fused biconical taper couplers. These optical fibre couplers are fabricated in industry by twisting together, melting and pulling two single-mode fibres around each other so that they get fused together over a uniform length called the coupling region as shown in Figure 4.1. The fibre cores are tapered and thinned out so that each core overlaps with the evanescent wave associated with light guided in the other mode which allows energy transfer [3].

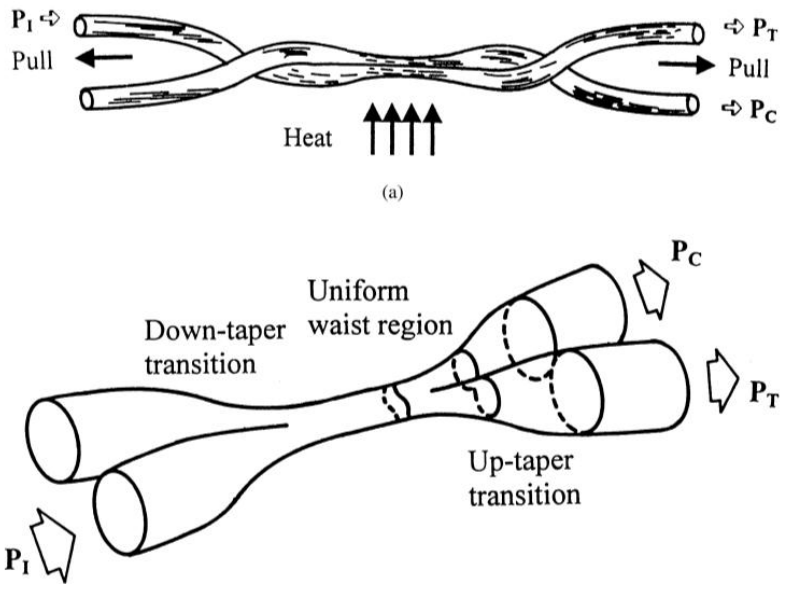

Figure 4.1. Fabrication method for a fused biconical tapper. The output ports are denoted by P_T and P_C [4].

The delay in Alice establishes a phase reference for the quantum state set by the phase modulator in the short arm while the equal delay in Bob allows for interferometric recombination of photons which have taken different paths at the final beamsplitter. A histogram of the time of arrival of photons travelling through the system is shown later in Figure 4.29. Only the photons which have travelled through the short arm in Alice and the long arm in Bob and vice versa undergo interference and the remaining two pulses are temporally gated out in software. The optical delay in Alice and Bob is created via a vernier controlled air gap. This allows fine adjustments to be made in the timing delay between the short and long arms in the interferometer which slightly relaxes the required accuracy that must be obtained when splicing to ensure that the nominal interfering peaks are temporally overlapping to within the coherence length of the laser. A variable air gap (OZ Optics ODL-200) was selected over a fibre stretcher

because of the superior optical delay which can be created with the air gap, which is a maximum of 3 cm in the system described here, which compares to a few mm in a fibre stretcher. Asymmetric double Mach-Zehnder designs in QKD systems commonly employ an active phase modulator (Photline NIR-MX800-LN-10)) at Bob to perform a basis set selection. However, this active component can induce thermal instability in the system and affect long term operation. The system described here employs two unbalanced Mach-Zehnder interferometers at Bob, one for each of the two basis sets, in order to improve thermal stability and to enable long-term continuous usage. To prevent environmentally induced changes in the birefringence of the fibre quantum channel from affecting the polarisation state of the transmitted photons, Alice scrambles her polarisation via a depolariser. A polarisation beamsplitter (PBS) (OZ Optics PBS) in Bob allows him to passively and randomly select what basis set he should make his measurement in. The operation of the depolariser together with the PBS in Bob is discussed in more detail in section 4.1.4. The QKD system was designed to be robust against externally induced changes in the relative path-lengths of the interferometers. During secure key exchange Bob continually monitored the visibility of his interferometers. Once the QBER exceeded a threshold level, typically 11%, key exchange was halted, and Alice's attenuation was reduced until pulses were transmitted which on average contained more than one photon. At this point Bob varied the relative path length delay of his interferometers using a computer controlled piezo-electric variable length air gap in the delay arms until the visibility was improved. This was achieved using fully automated custom tuning software which adjusted the piezoelectric voltage to restore good visibility. Alice then returned the attenuation to the correct mean photon per pulse level (μ) and key exchange was resumed. A μ value of 0.1 photons per pulse was used during all periods of key generation and Alice regularly monitored the μ value launched into the quantum channel and adjusted the attenuation using an optical attenuator (OZ Optics ODL-100) as required to compensate for any mechanical drift in the laser alignment which could cause the power to fluctuate. The μ choice of 0.1 means that approximately 5% of the non-vacuum pulses leaving Alice contained in excess of one photon, leaving it susceptible to the photon number splitting attack. The use of a μ value with known, controlled variances, known as decoy states, could be used to help increase the security of the system and this method has already been demonstrated at GHz clock rates [5].

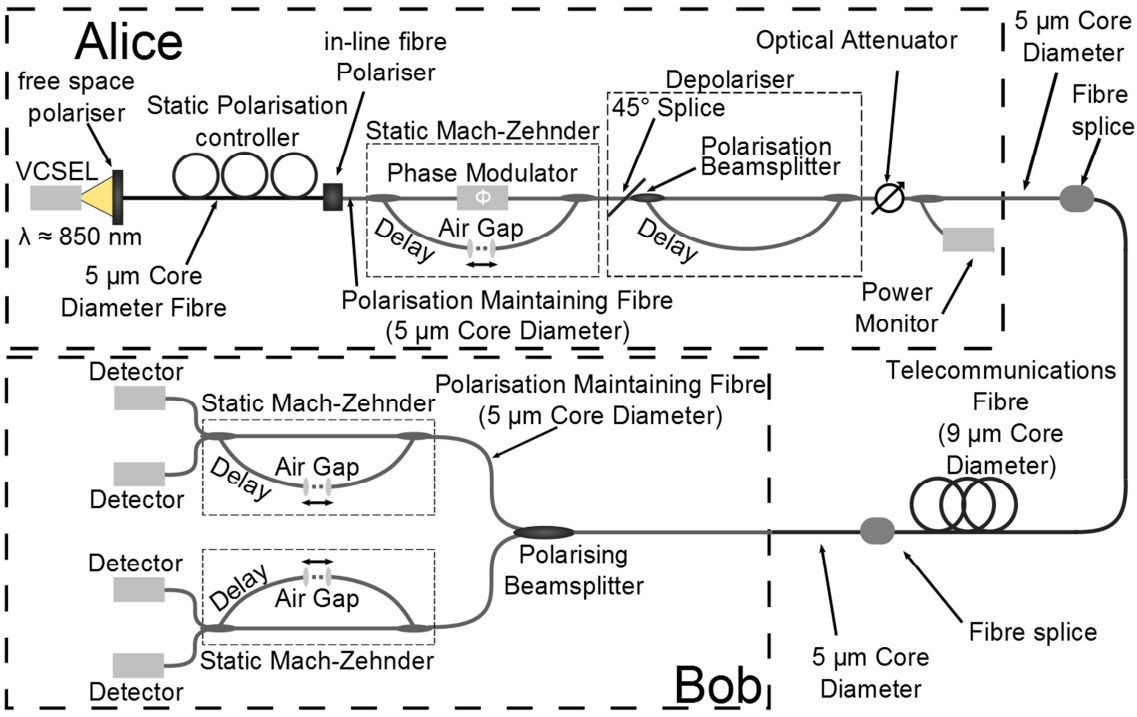

Figure 4.2. A schematic of the environmentally robust QKD system. The air gap in the transmitter is fixed for the duration of a measurement while those in receiver are adjusted under computer control to maintain the maximum fringe visibility in each interferometer.

The quantum communication channel is standard 9 µm diameter core Corning SMF-28e [1]. Operation at a wavelength of 850 nm requires mode manipulation techniques as 9 µm diameter core fibre can support more than one longitudinal mode. As described in Chapter 3 short lengths of 5 µm core diameter fibre are spliced onto the ends to spatially filter higher order modes.

4.1.2 Vertical cavity surface emitting laser (VCSEL)

The light source which was used in the system was a Honeywell HFE4093-322 vertical cavity surface emitting laser (VCSEL) operating at a wavelength of ~850 nm [6]. VCSELs are ubiquitous in modern long haul communications systems due to their low cost, low power consumption, high modulation rates and single-longitudinal mode operation [7]. The VCSEL was capable of operating at 2.5 Gbits/sec but was operated at 1 GHz to avoid excessive temporal intersymbol interference [8]. A spectrum of the laser output at various operating temperatures is shown in Figure 4.3.

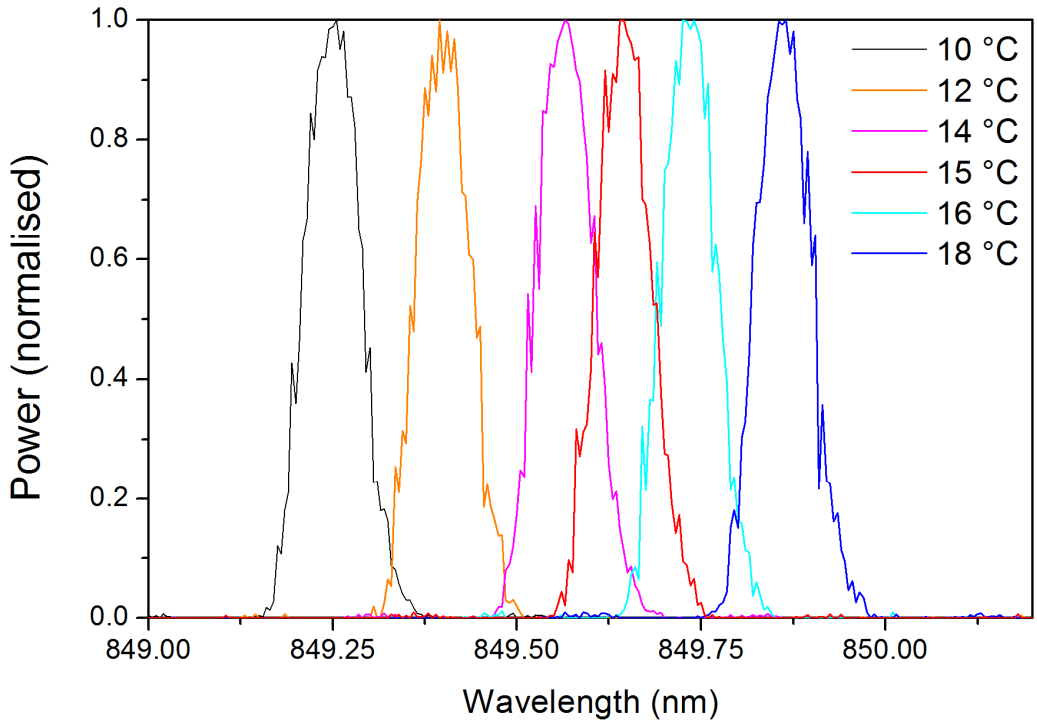

Figure 4.3. The spectrum of the Honeywell HFE4093-322 VCSEL when maintained at various temperatures using a peltier cooler.

The laser had a temperature dependent central wavelength of emission as shown in Figure 4.3 and Figure 4.4, and was determined to have a $\Delta\lambda/\Delta T$ of 0.0773 nm/°C. With increasing temperature the gain spectrum and the Fabry-Perot (FP) resonance of the cavity are red-shifted. The FP cavity resonance is determined by the temperature dependence of the refractive indices while the gain spectrum shift is due to the temperature dependence of the bandgap [9]. This required that the VCSEL be maintained at a constant temperature via a peltier cooler. A temperature of 15 °C was chosen as the operating temperature to try to maintain thermal equilibrium with the laboratory which was maintained at 15 °C using an air-conditioning unit which also ensured that water condensation did not develop on the device. The stability of the lasing emission wavelength was also important as the splitting ratio of fused biconical tapers have a wavelength dependence which could affect the interferometric visibility, since the two interfering beams must be equal amplitude to ensure high visibility [10]. This is explained in more detail in section 4.1.3. The VCSEL also exhibits a temperature dependence on the laser threshold current resulting in the power output increasing or decreasing with fluctuating temperature.

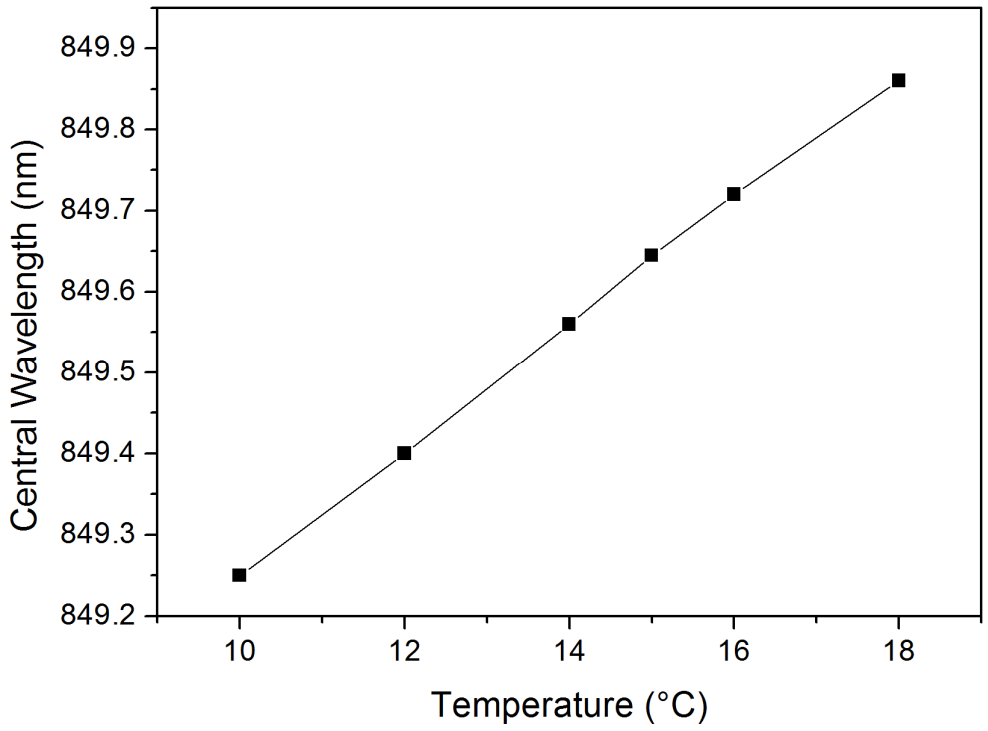

Figure 4.4. A Gaussian fit of the spectra peaks in Figure 4.1 is used to obtain the central wavelength. This wavelength is then plotted against the operating temperature maintained by the peltier cooler.

The full-width at half-maximum (FWHM) was measured to be 86.359 pm and the central wavelength was 849.64 nm at a temperature of 15 °C. This allows the coherence length of the laser, assuming it has a spectral broadening that is determined by a Gaussian process, to be calculated by

$$L_c = \sqrt{\frac{2\ln 2}{\pi}} \frac{\lambda^2}{\Delta\lambda} \qquad \text{Equation (4.1)}$$

where λ is the central wavelength and $\Delta\lambda$ is the spectral FWHM [11]. The calculated value was determined to be ~5.5 mm (corresponding a coherence time 18.52 ps in free space).

A short duration optical pulse is required to minimise the effect of timing jitter in the system, which could result in temporal intersymbol interference, resulting in bits being encoding incorrectly. A short duration optical pulse was achieved by the technique of gain switching in which a relatively long duration electrical driving signal can produce a much shorter temporal optical pulse [12], [13], [14]. In this method the threshold for laser oscillation is first obtained by the characteristic luminosity-current (L-I) curve for

the VCSEL. Figure 4.5 shows the L-I curve for various temperatures in the range 8-28 ºC. In edge emitting semiconductor lasers the threshold current I_{th} is given by

$$I_{th} \propto \exp\left(\frac{T}{T_0}\right) \qquad \text{Equation (4.2)}$$

where T_0 is the characteristic temperature. This shows that increasing temperature increases the threshold current.

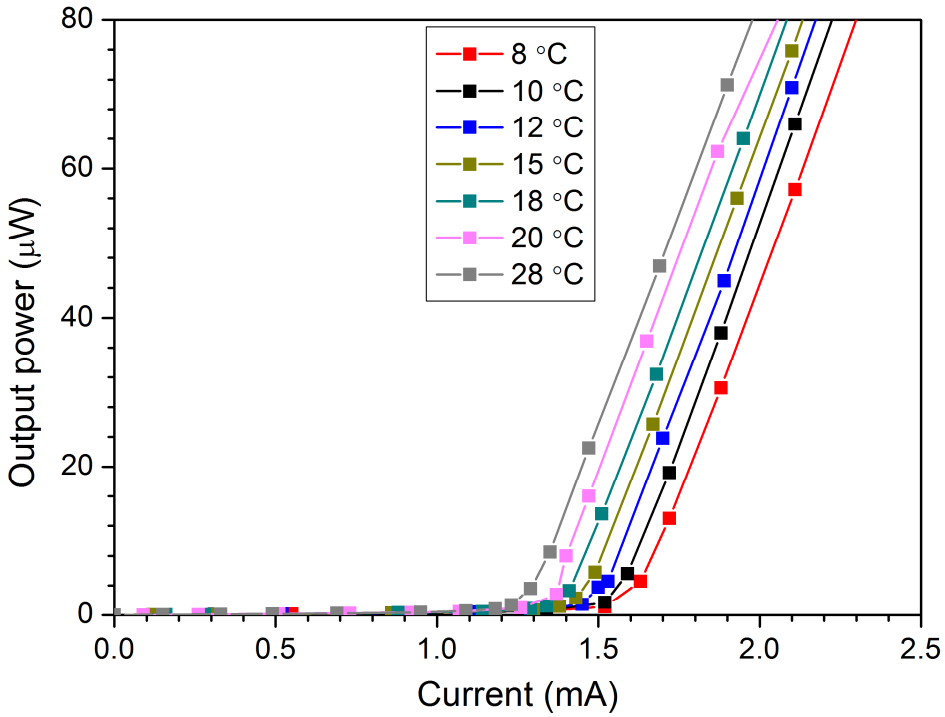

Figure 4.5. Characteristic L-I curve for the Honeywell HFE4093-322 VCSEL operating at various temperatures. When operated at a temperature of 15 ºC the threshold for laser operation was approximately 0.94 mA.

However as can be seen in Figure 4.5 and Figure 4.6, the threshold current temperature dependence is affected by the temperature range in which the laser is operating. This is caused by the laser gain spectrum and FP resonator modes shift to longer wavelengths at different rates as the temperature increases. Depending on the initial location of the gain peak with respect to the emission wavelength, the laser gain will either decrease or increase as the gain peak and emission wavelength slip into or out of alignment [15], [16]. The optimal temperature for alignment between the gain spectrum and FB resonator modes for the VCSEL studied here occurs at 45 ºC, where the laser threshold reaches a minimum. However operation at this temperature exceeds the manufacturers

recommended operating regime. When operated in the QKD system at 15 ºC the measured slope efficiency of the VCSEL was 0.14 mW/mA and the threshold for laser oscillation was approximately 0.94 mA.

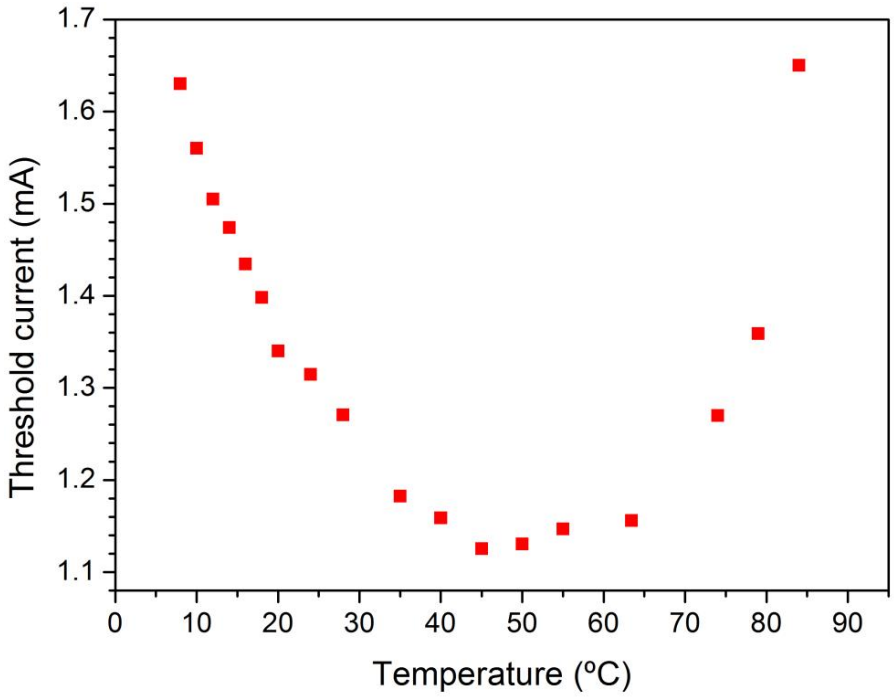

Figure 4.6. Variation in the threshold current for laser oscillation against temperature.

The schematic for gain switching is shown in Figure 4.7. The VCSEL was operated below the drive current for laser oscillations to occur by applying a constant DC current via a bias Tee (Picosecond Pulse Labs 5575A Bias-T). The gigahertz modulation signal was then provided by a pulse pattern generator through the bias Tee. The bias Tee consists of a capacitor and an inductor and is used to supply a DC offset to an AC signal. The capacitor represents a low-impedance path for the RF signal and a high impedance for the DC signal while the inductor offers a low impedance path for the DC signal and a high impedance for the RF signal [17]. The quality of the optical pulse was examined using a 12 gigahertz fast p-i-n photodiode on a 2.75 GHz bandwidth oscilloscope. Ideally in a QKD system the duration of the optical pulse should be as short as possible, with a clear distinction between the on and off state and also there should be no obvious double pulsing which broadens the temporal FWHM. Various conditions of the DC drive current, the width of the electrical driving signal and its voltage amplitude were investigated to obtain the optimal drive conditions.

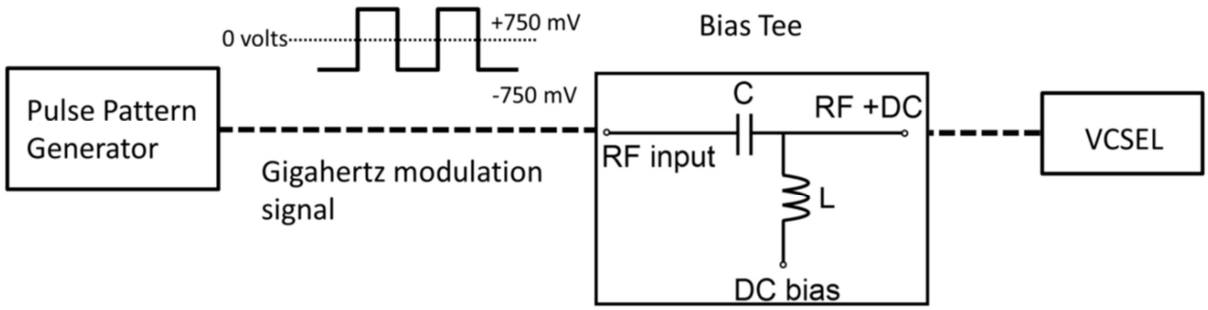

Figure 4.7. A schematic showing the arrangement for gain switching. The VCSEL is operated just below laser threshold via the DC current. A pulse pattern generator (PPG) provides the gigahertz modulation signal.

Figure 4.8 shows the electrical driving signal output form the pulse pattern generator used to pulse the VCSEL under optimal gain settings. The 1 GHz signal has a peak-peak amplitude of 1.5 volts and a FWHM of 503 ps.

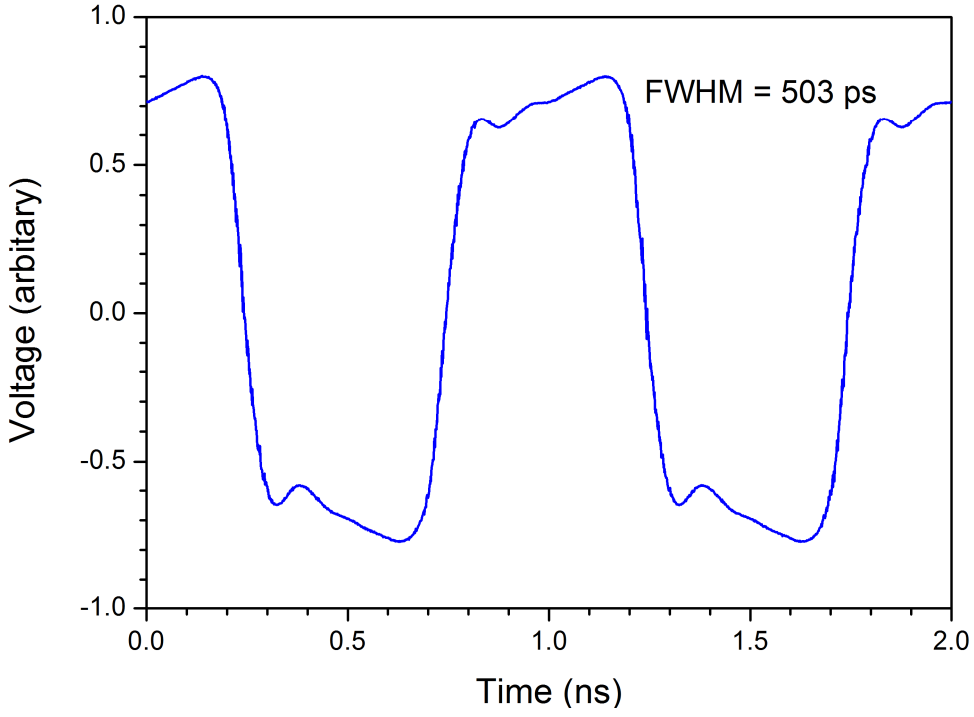

Figure 4.8. 1 GHz, ±750 mV peak-peak electrical driving signal for the VCSEL under optimal gain settings. The FWHM was measured to be 503 ps.

The DC current applied through the bias Tee was 0.5 mA. Figure 4.9 shows the temporal response of the VCSEL measured using a fast p-i-n photodiode and a

gigahertz oscilloscope. The insert shows the VCSEL temporal profile under gain switching settings that have not been optimised.

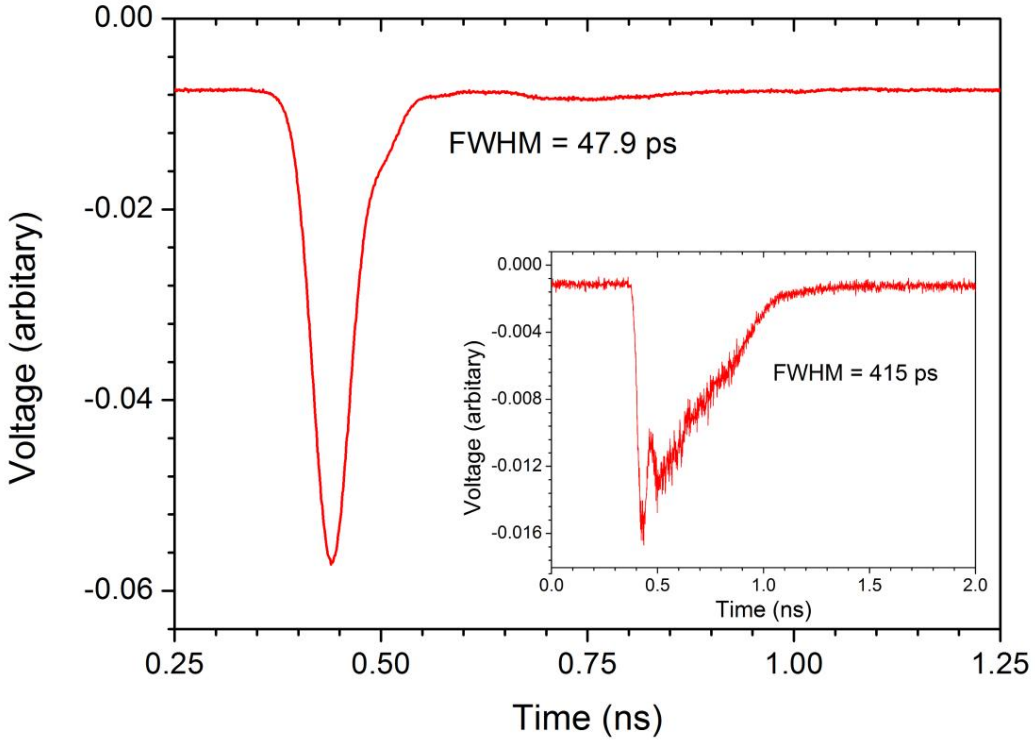

Figure 4.9. The temporal profile of the VCSEL on a fast p-i-n photodiode displaying a FWHM of 47.9 ps under optimal gain switching settings. The insert shows gain switching settings which have not been optimised using a DC current of 0.8 mA and a 1 GHz electrical driving signal of ±1000 mV with 50% duty cycle.

4.1.3 Polarisation of vertical cavity surface emitting laser (VCSEL)

The performance of any interferometric system depends greatly on the polarisation of the interfering beams [18], [19]. For two plane waves whose electric fields are given by

$$\vec{E}_1(\vec{r},t) = \vec{E}_{01}\cos\left(\vec{k}_1\cdot\vec{r}-\omega t+\delta_1\right)$$
$$\vec{E}_2(\vec{r},t) = \vec{E}_{02}\cos\left(\vec{k}_2\cdot\vec{r}-\omega t+\delta_2\right) \qquad \text{Equation (4.3)}$$

The result intensity $I=\left\langle \vec{E}^2\right\rangle_T$ when they undergo interference in a point in space is given by

$$\begin{aligned} I = E^2 &= \left(\vec{E}_1+\vec{E}_2\right)\cdot\left(\vec{E}_1+\vec{E}_2\right) \\ &= \vec{E}_1^2+\vec{E}_1^2+2\vec{E}_1^2\cdot\vec{E}_1^2 \\ &= I_1+I_2+I_{12} \end{aligned} \qquad \text{Equation (4.4)}$$

The term $I_{12} = 2\vec{E}_1^2 \cdot \vec{E}_2^2$ is referred to as the interference term. If the plane waves are perpendicular to each other, then the term $I_{12} = 0$, due to the dot product of the electric field vectors. When the plane waves are parallel then Equation (4.4) is simplified to

$$I = I_1 + I_2 + 2\sqrt{I_1 I_2}\cos\delta \qquad \text{Equation (4.5)}$$

where δ is the phase difference between the waves. Depending on the value of δ either constructive or destructive interference is observed. The visibility of the resulting fringes can be given by

$$V = \frac{I_{max} - I_{\min}}{I_{max} + I_{\min}} \qquad \text{Equation (4.6)}$$

where $I_{\max}$ and $I_{\min}$ are the light intensities of constructive and destructive fringes respectively. The visibility of the fringes is decreased by the factor $\cos\psi$ where ψ is the angle between the interfering electric fields. For maximum fringe visibility the intensity of the two interfering waves should be equal such that $I_1 = I_2$. In the case of the unbalanced Mach Zehnder interferometer in the QKD system, each arm usually has a different attenuation due to air gap losses, and in the case of Alice due to the loss of a phase modulator. The light which has travelled through the reference arm in Alice and signal arm in Bob and vice versa are made to have equal intensities by placing an adjustable screw attenuator into the air gaps in Alice's and Bob's interferometers which reestablishes the symmetry of the interfering pulses. However this technique has security implications as Alice sends a signal and references pulses with unequal amplitudes. The secure key rate is lower in this scenario than in the ideal case depending on the ratio of the reference pulse amplitude to the signal pulse amplitude [20].

The laser polarisation was investigated by sending collimated laser light through a free space polariser. The power output from the laser was monitored as a function of polariser angle and the resulting polar graph is shown in Figure 4.10. Two distinct transverse electric (TE) modes with roughly equal power are observed. The two modes arise from the fact that most VCSEL designs use circularly symmetric structures which results in no mode selection [21]. If the two orthogonal polarisation modes were allowed to remain they would degrade the visibility of the interferometry. A high

extinction ratio sheet polariser in excess of 10000:1 is used to remove this component leaving a single polarisation component as shown in Figure 4.11.

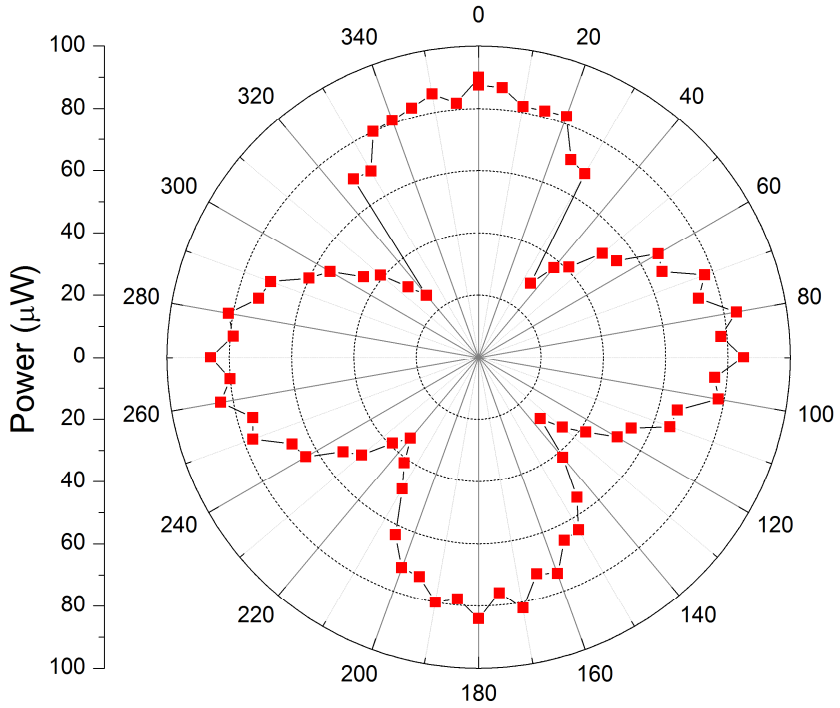

Figure 4.10. Polar graph showing the orthogonal polarisation components from the laser.

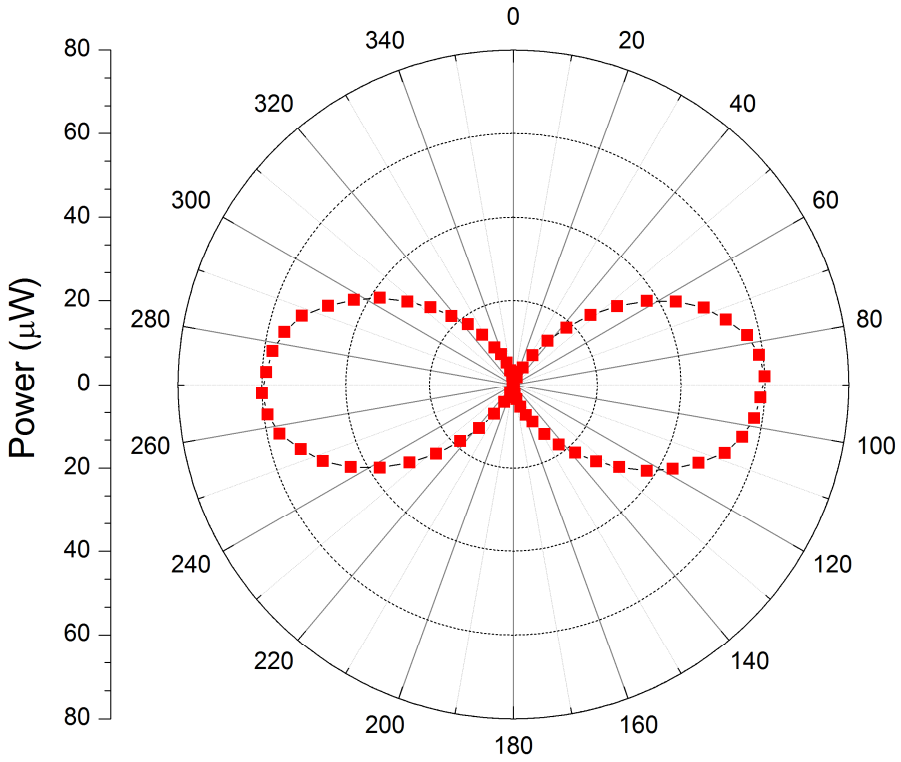

Figure 4.11. Polar graph showing the effect of the insertion of the high extinction ratio polariser to leave a single polarisation component.

Another common feature with VCSEL lasers is that the output polarisation can randomly flip axis [21] which can be an issue with PM fibres in which the light has to be correctly aligned with the stress members of the fibre. In Figure 4.2 after the laser light has been collected into the fibre, a static polarisation controller is used to correctly align its polarisation with an in-line fibre polariser. This ensures optimal polarisation alignment with PM fibres.

4.1.4 Operation of compact depolariser

The high clock rate quantum key distribution system is designed to be robust against environmentally induced fluctuations in the relative path lengths of the interferometers. The phase states for the implementation of the BB84 protocol are encoded using pulses of highly polarised light. However if the sender Alice was to transmit these encoded photons directly through standard telecommunications fibre, stress induced changes in the fibre birefringence would cause the polarisation to evolve randomly and thereby decreasing the visibility of the double Mach-Zehnder interferometers and increasing the QBER. However if the light emitted from Alice is fully depolarised then the effect of birefringence in the quantum channel can be eliminated. There are many various schemes which has been proposed in the literature for the implementation of such a device using either all fibre approaches [22], [23], [24] or bulk optics approaches [25], [26]. To be compatible with current fibre optic communications systems a fibre approach would be the preferred option to ensure successful integration into a QKD system. The compact fibre depolariser is based on a Mach-Zehnder type interferometer arrangement as shown in Figure 4.12 [25].

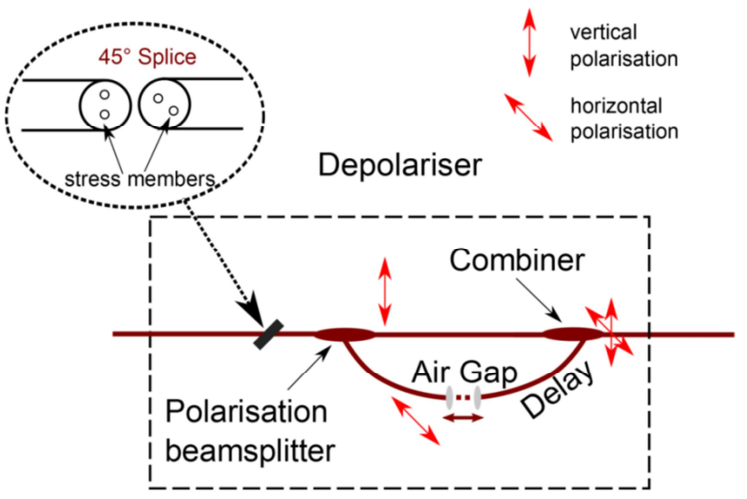

Figure 4.12. Schematic of the compact depolariser system with the 45° degree splice.

The depolariser was constructed using 5 μm core diameter panda eye polarisation maintaining fibre. The 45° splice at the input ensures that when polarised light is incident on the splice it equally excites two orthogonal polarisation modes in the fibre. The polarisation beam splitter then causes each polarisation mode to take different paths in the depolariser. In one of the arms an adjustable air gap allows the path separation to be adjusted. When the optical delay between the two arms in the depolariser is such that it is longer than the coherence time of the source and shorter than the optical pulse duration then when the two beams of light with orthogonal polarisations are combined at the final combiner, depolarised light is produced [25]. This effectively creates a differential group delay $\delta\tau_g$ which can be easily controlled by the adjustable air gap. This type of depolariser is capable of depolarising light sources with a relatively narrow linewidth (< 0.1nm). In the case of the all-fibre Lyot depolariser, which will be described in more detail in section 4.1.6, it relies on the differential group delay being created by the fibre length itself, which means that narrower linewidth sources require ever increasing lengths of fibre to fully depolarise them. The degree of polarisation (DOP) of the light exiting the depolariser was experimentally measured by monitoring the maximum and minimum power level detected when the light is analysed using a high extinction ratio polariser. The DOP can be analytically calculated as follows [27], [28].

$$DOP(\%) = \frac{I_{\max} - I_{\min}}{I_{\max} + I_{\min}} \times 100 \qquad \text{Equation (4.7)}$$

where $I_{\max}$ and $I_{\min}$ are the maximum and minimum recorded intensities after passing through a linear analyser. Completely polarised light has a DOP of 100% while unpolarised light has a DOP of 0%. The DOP and the polarisation output from the depolariser were investigated as a function of the path length difference between the arms of the depolariser. Figure 4.13 shows the DOP measured as a function of the analyser angle when the optical delay path between the two arms of the depolariser was identical. The two orthogonal polarisation components are still clearly visible and the maximum residual DOP is 82%. Figure 4.14 shows the DOP measured at an air gap separation of 20 mm which corresponds to a temporal separation of about 97 ps (refractive index of fibre core 1.4591 [29]) which is longer than the coherence time of the laser source. This demonstrates that the ratio of the polarised light to the total light intensity reduces to a value of about 11%.

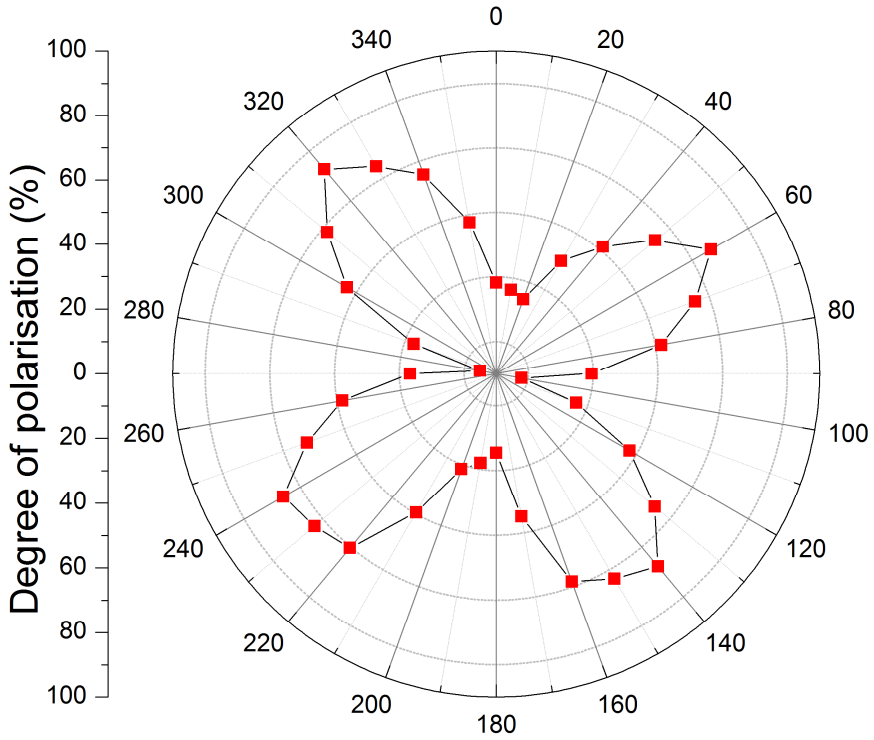

Figure 4.13. Degree of polarisation as function of analyser angle for a zero path length difference in the compact depolariser. DOP ≈ 82%.

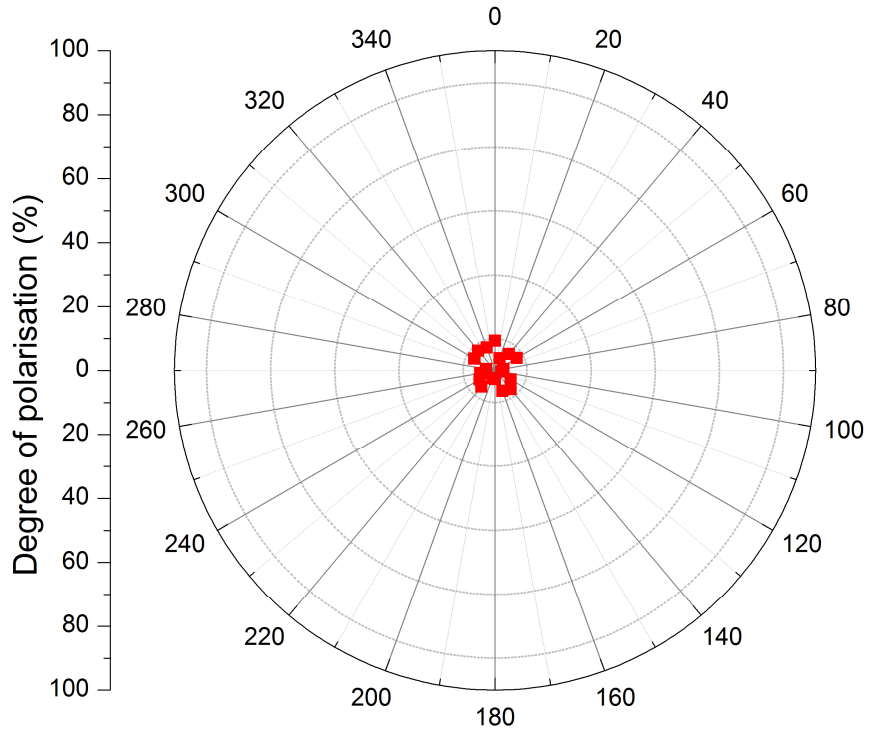

Figure 4.14. Degree of polarisation as function of analyser angle for a 20 mm path length difference in the compact depolariser. DOP ≈ 11%.

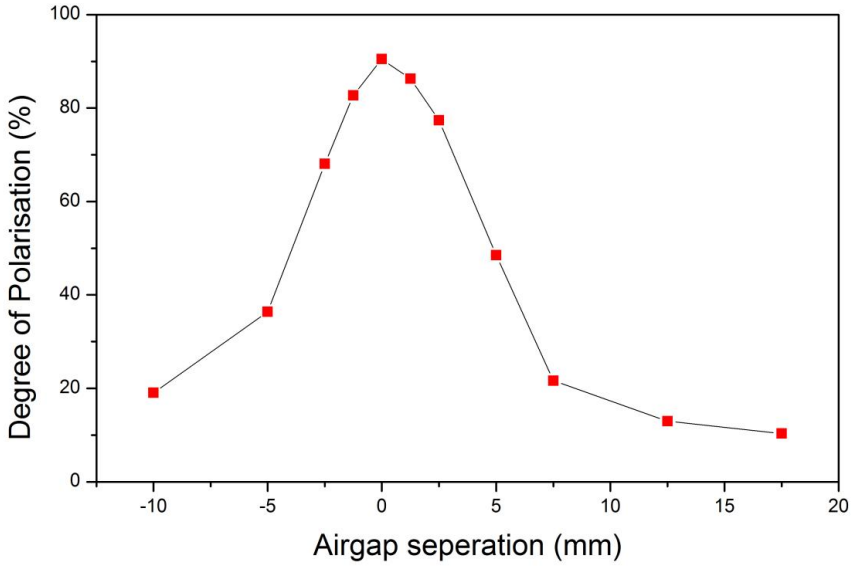

Figure 4.15. The variation of the degree of polarisation (DOP) as a function the air gap separation for a fixed analyser angle.

Figure 4.15 shows the variation of the degree of polarisation as a function of the air gap separation when analysed using a polariser with a fixed angle. At each delay position the light intensity was observed to fluctuate between a maximum and a minimum value when analysed with the polariser but this fluctuation ceased when the polariser was removed as the light intensity was measured on a free space optical detector which was insensitive to fluctuations in polarisation. At an air gap separation of 0 mm, which corresponds to a zero path length difference in the arms of the depolariser the light still contains a large fraction of polarised light. As the separation is increased the DOP decreases and it reaches a minimum value when the separation is longer than the coherence length which was calculated to be 5.5 mm when derived from the linewidth of the source. The coherence length can also be calculated from Figure 4.15 by using the half-width at half maximum which gives a value of 5.1 mm [30]. Deviations from the calculated value of 5.5 mm may be attributed to the finite number of points in Figure 4.15 when fitting the Gaussian linewidth and to the uncertainly in the measured value of the linewidth of the source.

4.1.5 Security consideration of depolariser

The depolariser allows light propagating through standard telecommunication fibre to be immune from birefringent effects in the fibre. Polarised light travelling in this channel would suffer a random evolution of its polarisation as a result of stress induced changes in the intrinsic birefringence in the fibre [31], [32], [33], and thus would require

active polarisation controllers at the receiver to ensure good interferometric visibility [34]. When integrated into the QKD system in Alice, the depolariser generates depolarised light which then travels through standard telecoms fibre and arrives at Bob the receiver. In Bob a polarisation beam splitter acts as a random routing component and it is by this method in which he randomly selects which basis set to make his measurement in. This method may produce a potential security loophole in which an eavesdropper may be able to exploit. If the eavesdropper was to intercept a photon emitted from Alice and then resend the photon with a particular polarisation, it is possible for her to force Bob to make a particular basis set measurement of her choosing. This would enable the adversary to gain additional information on the key. A potential solution to this problem would be to introduce a second depolariser into Bob before his polarisation beam splitter (PBS). This would hopefully guarantee that any light reaching Bob's PBS is depolarised ensuring that his basis set selection is completely random.

A design consideration which must be taken into account with the depolariser is its loss. A high optical loss in such a component (~10 dB in the case of the compact depolariser) in Alice is not a big issue when she is using a weak coherent source. It is possible for her to turn up her laser power to accommodate this loss but still ensuring a 0.1 mean photon number per pulse leaving her system. However if the depolariser were to be placed into Bob's apparatus then its loss would have a major bearing on the overall bit rate for the QKD system. In the next section a low loss Lyot depolariser is discussed which can in some ways alleviate this problem.

4.1.6 Lyot depolariser

An alternative to the compact depolariser is to use an all fibre Lyot depolariser [35]. In its original design conception in 1929 it consisted of two birefringent crystals with a 2:1 thickness ratio in which the optic axes are orientated at 45° to each other [36]. It was designed originally to work with a broadband light source. Depolarisation is produced by the different wavelength components of the source suffering unequal phase retardation as it travels through the crystal [37], [30]. The fibre Lyot depolariser works in a similar fashion, the two birefringent crystals are replaced by two lengths of polarisation maintaining (PM) fibre which are spliced together at an orientation of 45° as shown in Figure 4.16. The requirement of the fibres having a specification length ratio is removed if the input light is polarised and aligned with the birefringent axis or stress member of the input fibre [30].

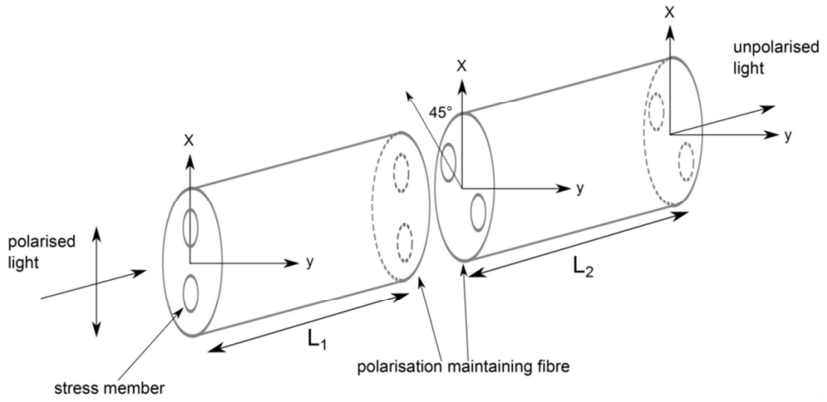

Figure 4.16. All fibre Lyot depolariser built from two polarisation maintaining fibre spliced with their stress members at an angle of 45º.

The output degree of polarisation for the Lyot depolariser for a Gaussian spectral shape is given by

$$\gamma(z) = \exp\left[-\left(\frac{\delta\omega\delta\tau_g z}{2\sqrt{\ln 2}}\right)^2\right] \qquad \text{Equation (4.8)}$$

where $\delta\omega$ is the spectral half-width at half maximum, $\delta\tau_g$ is the differential group delay and z is the length of the second jointed fibre [37].

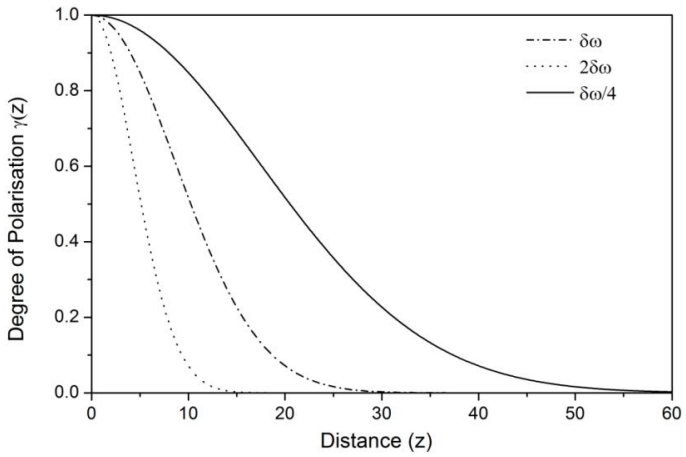

Figure 4.17. The predicted degree of polarisation as a function of the distance which was modelled using a half-width at half maximum $\delta\omega$ of 0.2×10^{12} Hz and a differential group delay of 1.35×10^{-9} ns/m.

Figure 4.17 shows the effect of the spectral linewidth $\delta\omega$ of the source has on the degree of polarisation. It shows that the Lyot depolariser requires ever increasing lengths of fibre to achieve the same degree of polarisation for narrower linewidth sources. The Lyot depolariser also suffers a potential security loophole which can be exploited by an Eavesdropper. Like in the case of the compact depolariser the ability of

the PBS to act as a random routing component requires depolarised light at its input. The DOP of the Lyot can be increased by an eavesdropper in an intercept-resend attack by decreasing the spectral width of the light thereby having control over Bob's basis set measurement. However, as in the case of many security loopholes, this issue may be resolved if Bob monitors the coherence length of the source which can be measured using interferometric techniques in which he adjusts the path length different to determine the FWHM of the interferometric fringe pattern [38].

4.1.7 Effectiveness of the compact and Lyot depolariser

In an ideal situation when depolarised light is incident at the PBS in Bob it is randomly routed into one of Bob's two interferometers for his basis set measurement. However due to optical imperfections in the QKD system the light still possesses a residual amount of polarisation and hence will affect the 50:50 splitting ratio at the PBS due to polarisation fluctuations. To test the effectiveness of each depolariser, polarised light was passed through the depolariser and sent through the PBS. The photon count rate on the two output ports of the PBS (port 1 and port 2) was monitored using two single-photon detectors. Figure 4.18 shows the effectiveness of the all fibre Lyot depolariser when its length was 100 metres. Port 1 and port 2 show the count rate on the two output ports of the PBS. The symmetry of the photon count rate on the output of the PBS is apparent. As the photon count rate on port 1 increases the corresponding count rate on port 2 decreases due to polarisation evolution of the light. It is also possible to see a direct correlation between the photon count rate, on both channels, with temperature. When the temperature begins to increase or decrease a corresponding fluctuation in the photon counts rates may be observed which suggests the primary source of polarisation evolution is due to temperature variations in the environment. Temperature sensors were located both inside and outside the box containing Bob. At a length of 100 metres the Lyot depolariser was not particularly effective showing a residual DOP of about 25% as shown in Figure 4.18. When this length was doubled to 200 metres a dramatic reduction was observed in the DOP to about 7% shown in Figure 4.19. At this length the Lyot appears to be even more effective than the compact depolariser in Figure 4.20 which had a DOP of 10%. The 200 m Lyot depolariser has also the added benefit for having a loss of about 1.5 dB in comparison to about 10 dB for the compact depolariser. When the depolariser was removed from the system and the PBS in Bob replaced by a 50:50 beamsplitter the recorded visibility of the interferometers dropped to 67% which

is equivalent to a QBER contribution of 16.5% which demonstrates the effectiveness of the depolariser and PBS arrangement.

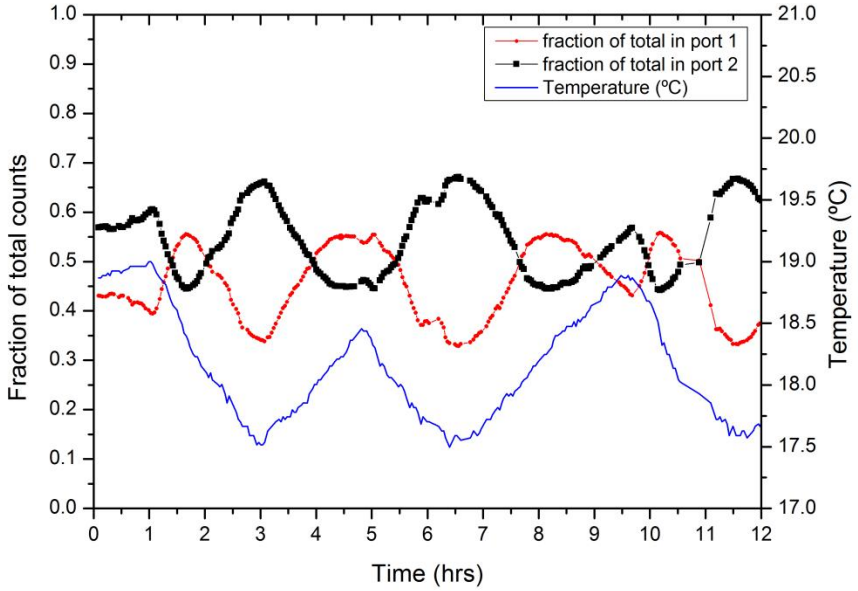

Figure 4.18. The Lyot depolariser with 100 metre fibre length. The left axis shows the count rate as a fraction of the total count rate across both channels. The photon count rate is monitored on the two output ports of the PBS. The right axis shows the temperature fluctuations over the measurement. The lowest standard deviation was 0.071 for a particular output port. Residual DOP was about 25%.

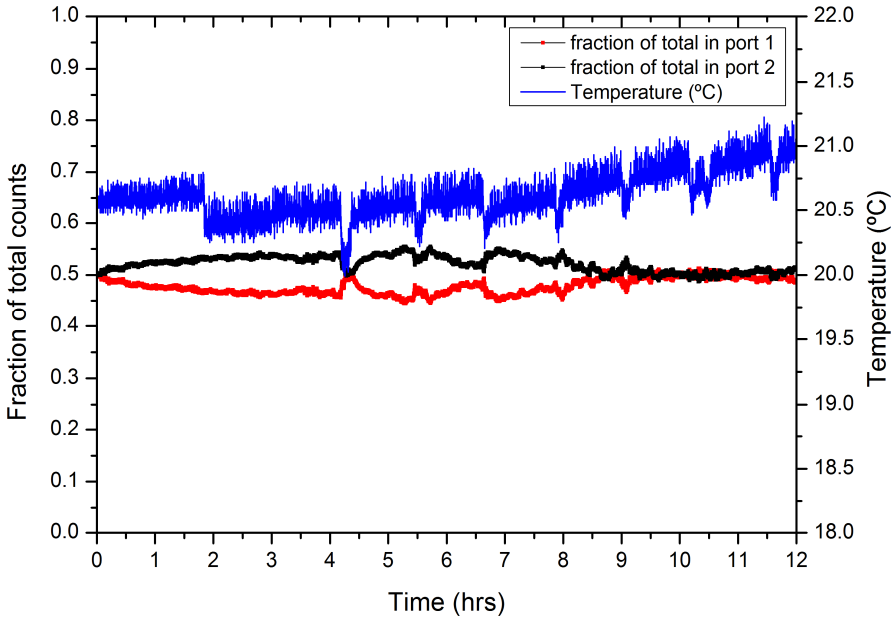

Figure 4.19. The Lyot depolariser with 200 metre fibre length. The left axis shows the count as a fraction of the total count rate across both channels. The photon count rate is monitored on the two outputs of the PBS. The right axis shows the temperature fluctuations over the measurement. The standard deviation was 0.0194. Residual DOP was about 7%.

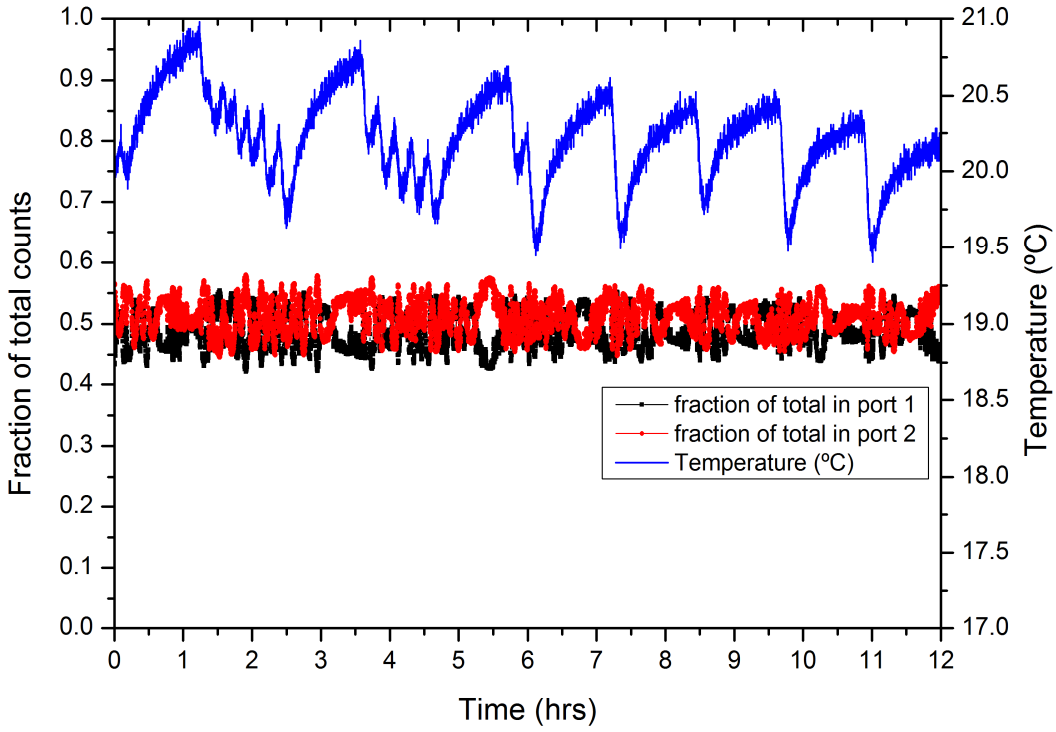

Figure 4.20. The compact depolariser. The left axis shows the count as a fraction of the total count rate across both channels. The photon count rate is monitored on the two outputs of the PBS. The right axis shows the temperature fluctuations over the measurement. The standard deviation was 0.0278. Residual DOP was about 10%.

4.1.8 Electronic and software for the QKS system

4.1.8.1 Time division demultiplexing

A key piece of hardware infrastructure is the conversion of the SPAD electrical signal to a time of arrival of a photon. The piece of electronic hardware which was used to time tag the arrival times of the photon was a time interval analyser (TIA) GT685 [39]. The GT586 has two independent timing inputs which poses a challenge for the implantation of the BB84 protocol for QKD which encodes information using four phase or polarisation states. This means that the timing information of four detectors is required for the system described here. The technique of time division multiplexing is used to allow timing information from all four detectors when only two designated timing inputs are available. This is implemented by splitting the electrical signal from each of the four detectors into two and then adding known delays of electrical cable into each delay arm. Each half is then fed into a four input logic OR gate (Philips 755 Quad 4 logic gate) whose output is then fed into the two timing inputs channels of the TIA. By looking at the delays between the two channels allows knowledge of which detector fired and its timing information. The process can be followed more closely in Figure 4.21. When the difference between the time tags on channel A and B is 0.8 ns then

SPAD 1 fired and likewise SPAD 2, 3 and 4 are identified by timing delays of 1.6, 2.4 and 3.2 ns respectively.

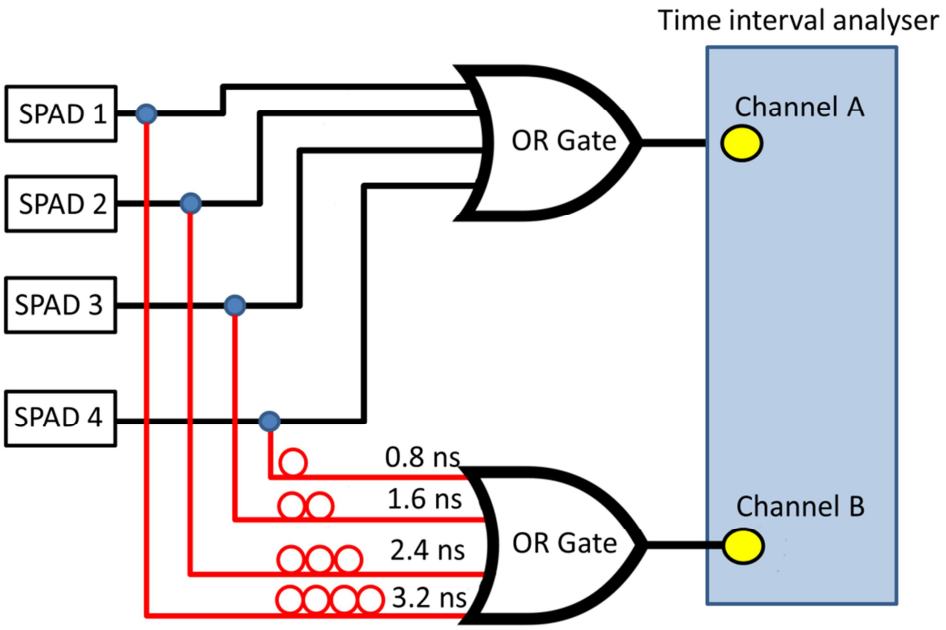

Figure 4.21. Schematic for time division multiplexing.

By histogramming the timing difference between the time tags on channel A and B, created when light is equally incident on all four SPADs, it is possible to observe four peaks in the histogram corresponding to the four timing delays which have a full-width at a hundredth-maximum of ~0.5 ns. The increments of 0.8 ns in the timing delay for each detector becomes more obvious from examining Figure 4.22. A delay of 0.8 ns means that the adjacent peaks are well separated temporally to avoid any ambiguity about which detector fired because of the timing jitter of the detector. The probability that dark counts in the detectors could cause simultaneous clicks is negligible. The joint detection probability for two detectors is given by

$$P(t_1 : t_2)\Delta t_1 \Delta t_2 = I(t_1) I(t_2) \Delta t_1 \Delta t_2 \qquad \text{Equation (4.9)}$$

where events occurs at times t_1 and t_2 in a window Δt_1 and Δt_2. $I_1(t_1)$ and $I_1(t_2)$ are the instantaneous light intensities [40]. In the case of two detectors with dark count rates N_1 and N_2, the probability of coincidence events in a time window Δt is given by

$$P(t) = N_1 N_2 \Delta t^2 \qquad \text{Equation (4.10)}$$

This probability already incorporates the dead time of the detector which is about 50 ns for a Perkin Elmer Si-SPAD. For a dark count rate of ~350 counts per second and a sub nanosecond time window $P(t) \approx 0$.

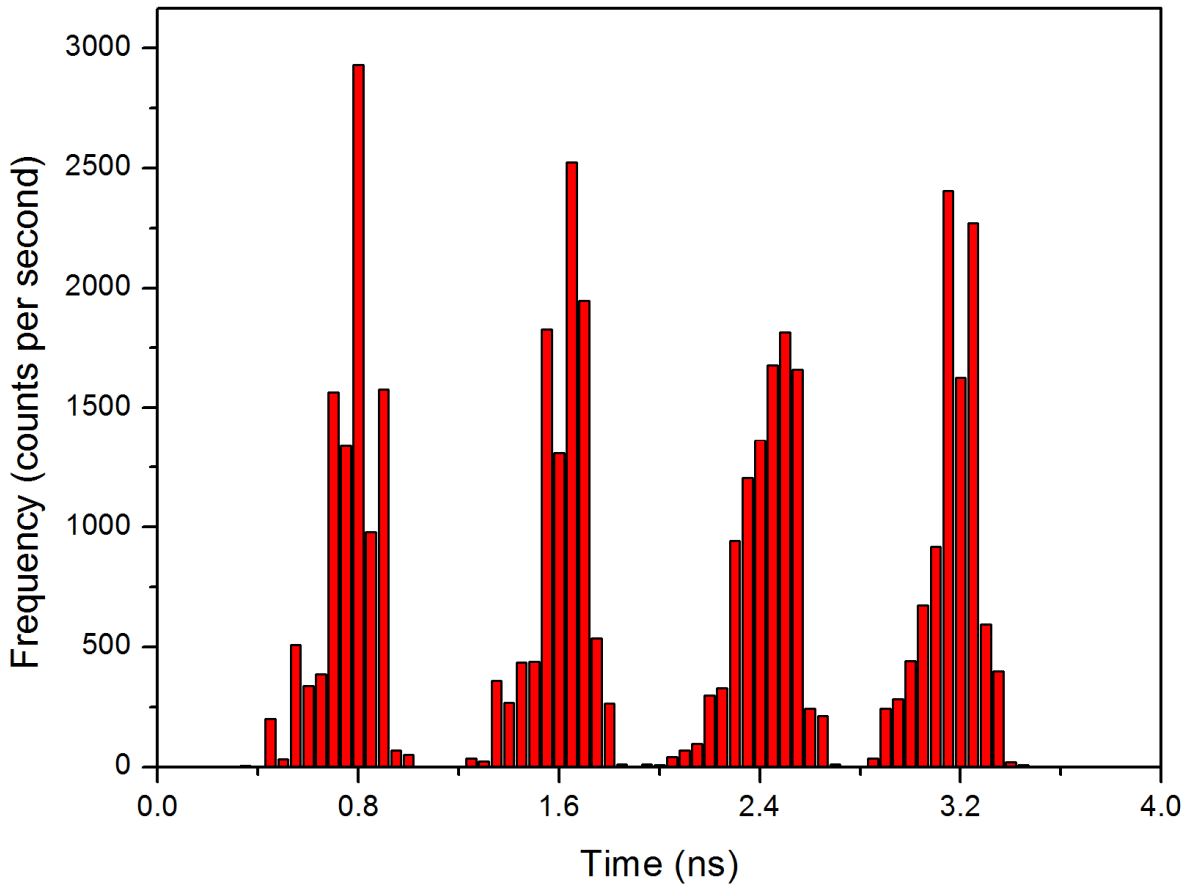

Figure 4.22. The result of histogramming the difference between the time tags on channel A and channel B on the time interval analyser card with equal light intensity falls on all four detectors. Four characteristic peaks are observed corresponding the delays of 0.8, 1.6, 2.4 and 3.2 ns.

4.1.8.2 Generation of 4 states for the BB84 protocol

The implementation of the BB84 protocol for QKD requires that Alice randomly encodes information using a "1" or a "0" chosen randomly from two basis sets. For the QKD system described here, this requires Alice being able to generate 4 different phase states. A pulse pattern generator (PPG) provides the electrical signal to the lithium niobate ($LiNbO_3$) phase modulator to generate the states. The phase modulator works via the electro-optic effect previously described in Chapter 3, whereby an applied electric field can change the refractive index n of the crystal thereby causing the speed of light c to vary according to c/n. The PPG has only two designated outputs which requires that the outputs be electrically combined at the output in addition to using a

data pattern the four voltages states can be produced. Channel 1 is set to a voltage of 0.8 volts which produces a phase shift of $\pi/2$ and channel 2 is set to produce a voltage of 1.6 volts which is the voltage required to produce a phase shift of π. As shown in Figure 4.23, by the choice of bit value being either on or off on channel 1 and channel 2, the four states required can be generated. The Avtech electrical power combiner (Avtech AVX-CP-2) has an electrical loss of 3 dB [41] which means the maximum the PPG can supply to the phase modulator through the combiner was 1.4 volts. This required that the output from the combiner be amplified using a Picoseconds Pulse Labs amplifier (Model 5866) to produce 2.4 volts to create the final state.

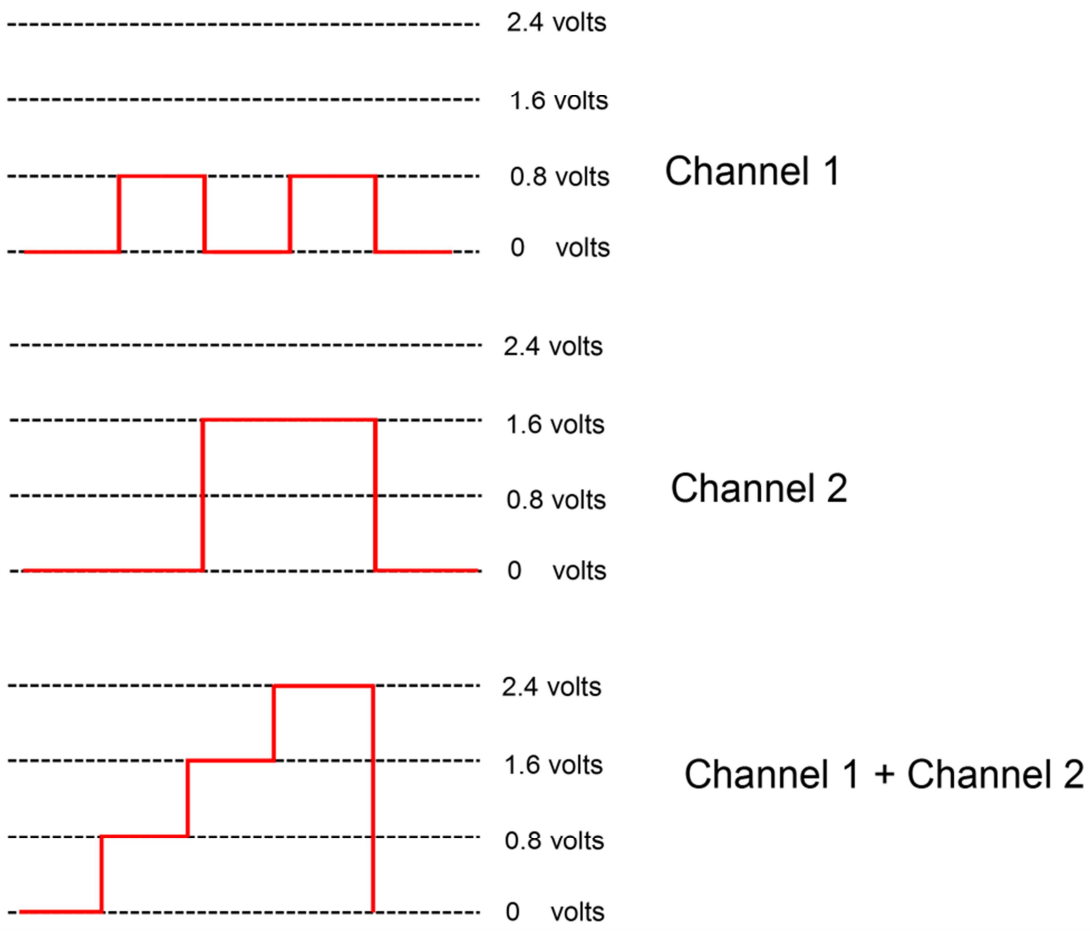

Figure 4.23. Diagram showing how a four level voltage system can be generated using a two output pulse pattern generator.

Figure 4.24 shows a typical electrical driving signal which is applied to the phase modulator to generate the four states. Electrical ringing can be observed in the signal especially when the voltage is being changed from a high to a low level. The amplitude

jitter can be as much as 8% of the voltage amplitude leading to phase encoding errors which will be described in more detail in section 4.2.1.

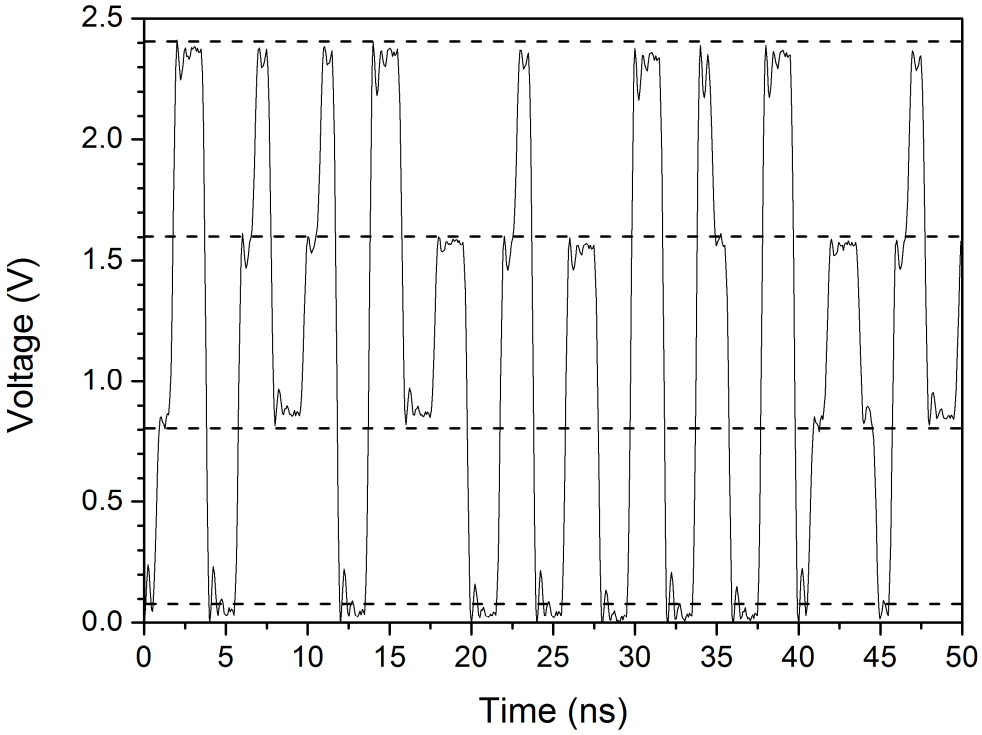

Figure 4.24. Graph showing a typical electrical driving signal to the phase modulator using a four level pseudo-random signal.

4.1.8.3 Pattern Matching

A 10 MHz Rubidium frequency (Novatech 2960 AR) standard acted as the master clock for the system and was used to the clock the Agilent 81134A pulse pattern generator (PPG). The frequency standard uses the hyperfine transition of electrons in an atom of Rb-87 to control the frequency. The ground state hyperfine splitting frequency is 683468261090429 Hz [42]. The output is used to apply an external clock signal for the internal phase lock loop in the PPG and also the time stamping card to ensure all devices are correctly synchronised. The PPG was then used to provide the 1 GHz electrical signal to drive the VCSEL and also to provide the 1 GHz signal to the lithium niobate phase modulator crystal. In QKD Alice sends encoded photons at precise time intervals to Bob who then detects the photon using a single-photon avalanche photodiode (SPAD). For final key generation to be successful it is necessary that when Bob records a photon event he must know precisely from what position in Alice's bit pattern the photon was sent. This synchronisation is often provided by a bright light pulse [43], [44] or by clock signals derived from the global positioning system (GPS) [45]. The approach adopted here is to use software synchronisation [46], [47] which

has the added benefit of not requiring additional synchronisation hardware. A pseudorandom bit sequence (PRBS) known to both parties can be used to synchronise Alice's and Bob's clock using pattern recognition techniques [48], [49]. The clock rate of the system is 1 GHz which means that Alice emits a photon at an integer times the clock period. Bob's rate of detector clicks will be dramatically reduced by the transmission distance, his detection efficiency and his measurement apparatus loss. Figure 4.25 shows a histogram of the photon arrival times at Bob when Alice sends a 32 bit pseudorandom pattern (00100100011101100110110010110011) that is used for synchronisation. The non-interfering pulses are still visible and are temporally gated in software as shown in Figure 4.26.

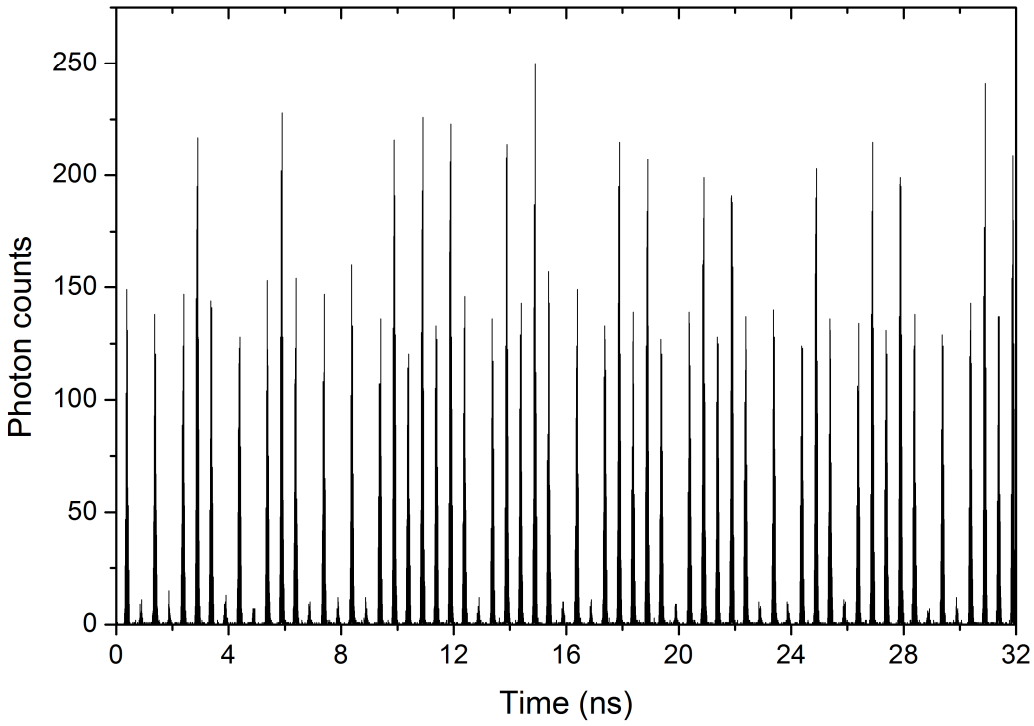

Figure 4.25. Histogram of a 32 bit, pseudo-random bit pattern sent by Alice. The non-interfering pulses are still visible.

The first bit in this pattern is not necessary the first bit sent from Alice. Due to the transit time of a photon traveling through the system the position of the first bit in Alice's pattern can be randomly distributed along the entire bit length of the pattern. In an ideal case the length of the bit pattern should be longer than the time it takes a photon to travel from Alice to Bob thereby eliminating the chances of more than one repeat of the pattern being in transit at any given time. A similar technique is used to avoid range ambiguity in time-of-flight laser ranging systems [50]. The software

operates as follows; a series of n windows (n is the length of the PRBS) of width ΔT and spaced by the clock period of the laser source is opened on the time tags recorded by Bob. The time tags which fall into each of the n windows are then rounded down to the nearest integer number corresponding to the clock period and a modular division by the length of the data pattern is performed. This essentially converts each recorded time tag to a bit timing position recorded by Bob. Alice and Bob already know the bit sequence for synchronisation and then compare their bit values and compute the QBER. Due to the transmission distance and the random time at which Bob's time stamping card starts acquiring data there will be an offset between Alice's and Bob's bit pattern. For a pseudorandom pattern in which Alice's sent pattern and Bob's received pattern are not synchronised correctly the QBER should be approximately 50%. In the case where there is no synchronisation Bob then increments each of his recorded bit times by one position and repeats the comparison with Alice. This procedure is repeated $n-1$ times. The result of this process is shown in Figure 4.27. At one position the QBER reduces dramatically which indicates that Alice's and Bob's pattern have been correctly locked. The whole procedure can be thought of as a correlation between Alice's and Bob's signals.

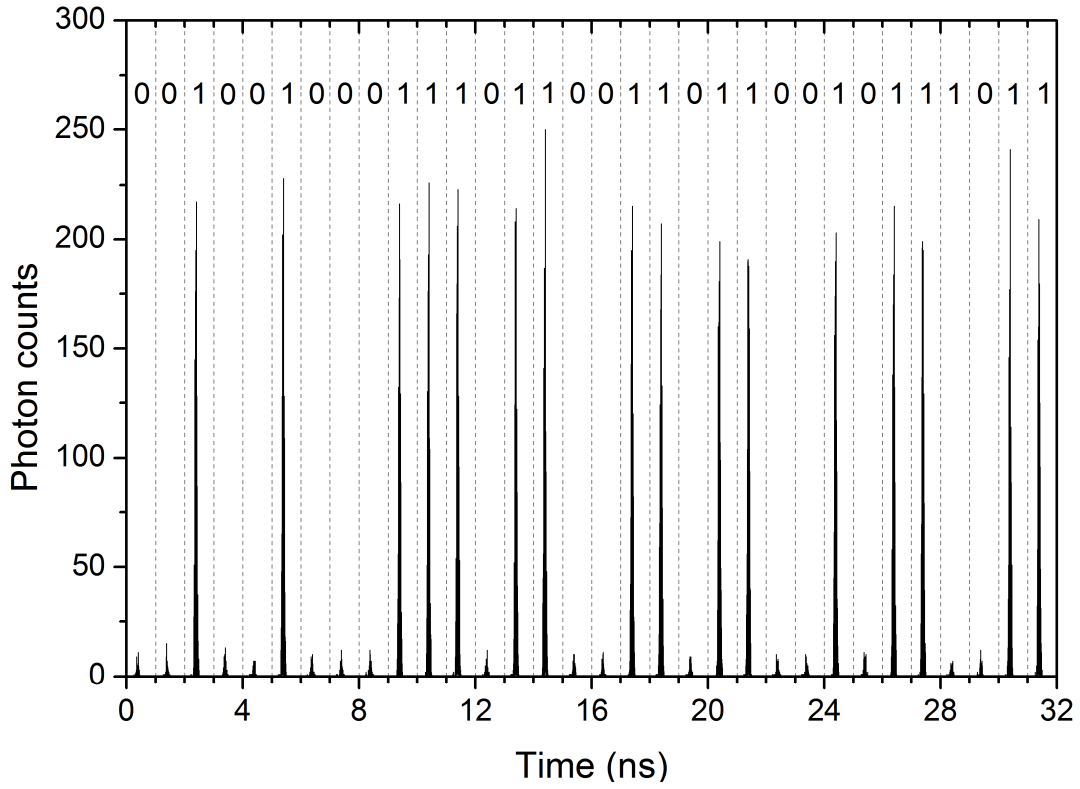

Figure 4.26. Histogram of the time of arrival of photons sent by Alice. The non-interfering pulses have been temporally gated using software control making the PRBS of 00100100011101100110110010110011 more distinguishable.

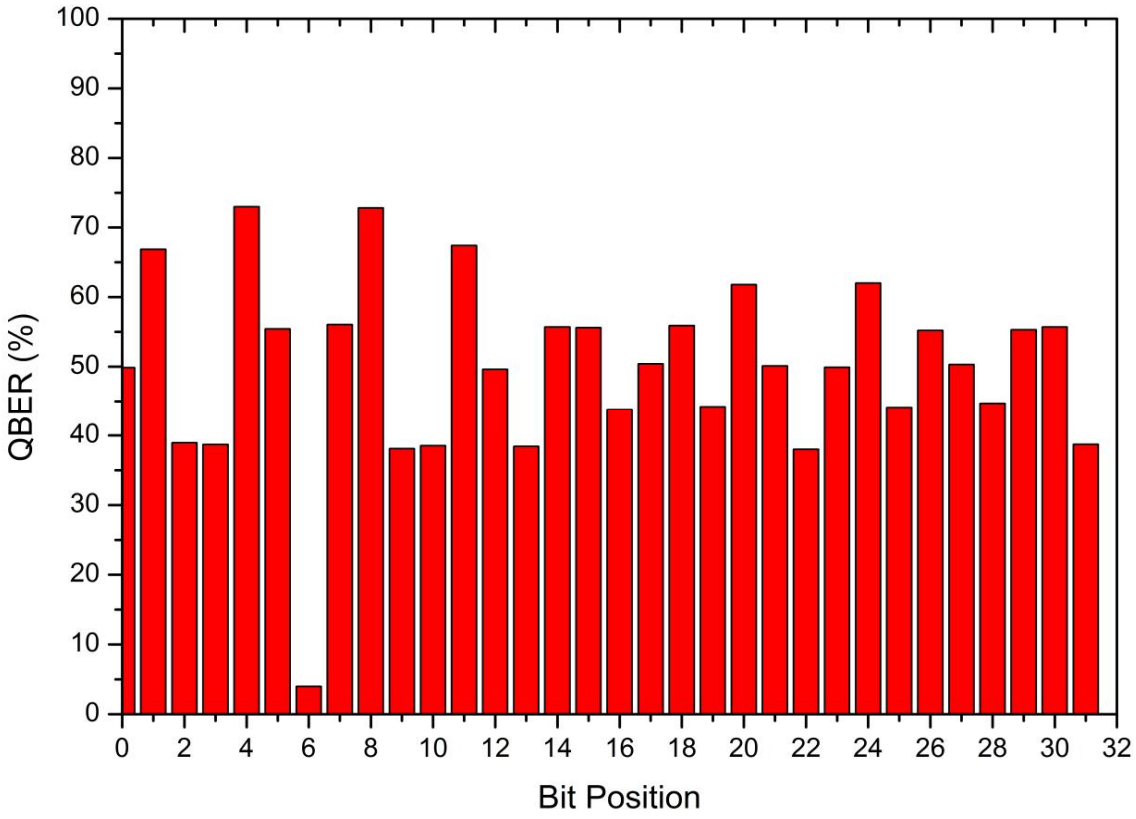

Figure 4.27. Output from the program to synchronise Alice's and Bob's clocks. When the value of Bob's timing bits are offset by 6 bits in this example there is a dramatic reduction in the QBER enabling a synchronisation between Bob's and Alice's clocks.

4.2 Results and theoretical evaluation of QKD system

The QKD system described in this chapter was tested with a variety of single-photon detectors which have reasonably good detection efficiencies at a wavelength of 850 nm. The characteristics of these detectors have a significant bearing on the overall system performance of the QKD system in which they are used. A number of previous demonstrations of QKD at a wavelength of 850 nm have used thick junction Si-SPADs as the detectors [44], [51]. These detectors have the advantage of having good detections efficiencies of about 40% at this wavelength but they do suffer from a relatively long timing jitter with a full-width at half maximum of about 400 ps. This timing jitter can lead to temporal intersymbol interference especially when the system is operated at clock rates in excess of 1-2 GHz [52]. This results in photons being recorded in successive bit periods as the timing jitter can exceed the clock period. Thin, or shallow, junction Si-SPADs have the benefit of shorter duration FWHM timing jitters of about 70 ps but can exhibit long tails in their timing profile caused by relatively slow diffusion of photo-generated carriers into the device multiplication region [53]. These diffusion tails can be characterised by the full-width at 10^{th}-maximum (FW10%M) and

full-width at 100th-maximum (FW1%M) timing jitters, and can be observed in the timing histograms shown in Figure 4.28 and shown numerically in Table 4.1. These thin junction detectors generally have reduced detection efficiencies of <10% at this wavelength.

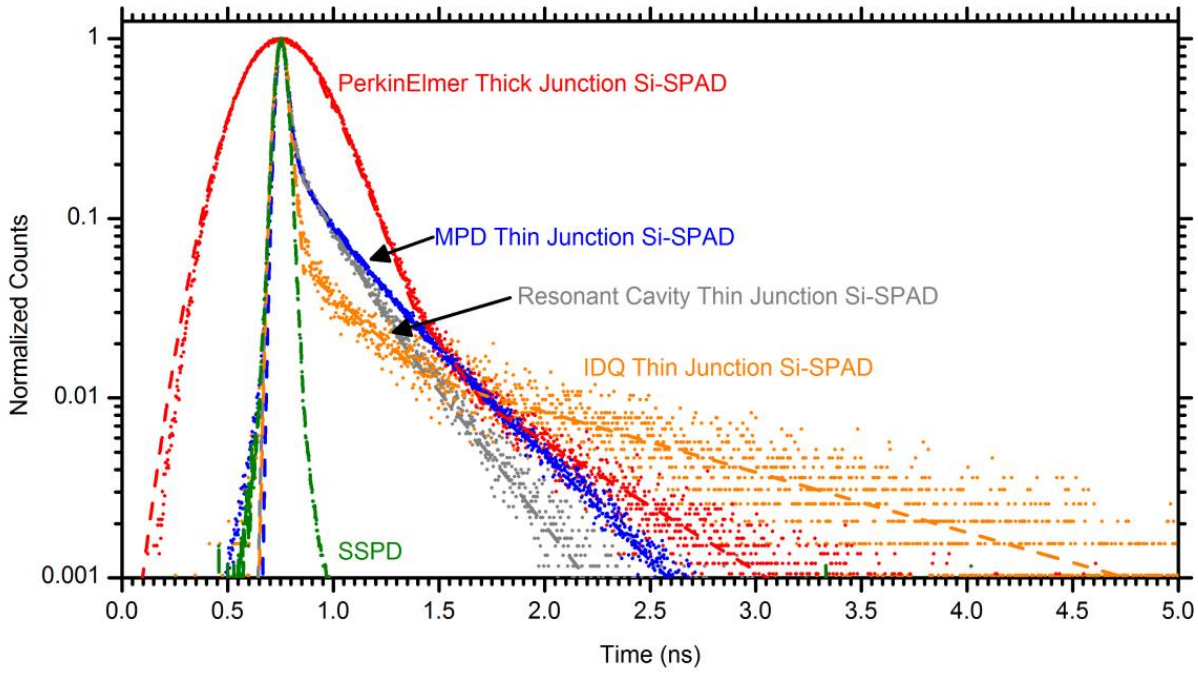

Figure 4.28. The normalised instrument responses for the specific detectors when used in the QKD system. The dashed lines represent a piecewise exponential fit used in the theoretical model. (SSPD is the single-photon superconducting nanowire detector)

The detection efficiency of a thin junction Si-SPAD may be improved without compromising the temporal response and dark count rate by the use of a resonant cavity to increase the effective interaction length for absorption of incident photons [54]. The lower mirror of the resonant cavity is formed by the two layers of buried SiO_2 in the silicon substrate, and the upper mirror is formed by the silicon/air interface. The upper, low-doped p-epilayer contains the active n^+p-junction of the detector with an active area of 20 µm diameter. The complete epilayer structure had a thickness of 5 µm. In Figure 4.28 it can be seen that the resonant cavity and the thin junction Si-SPAD from Micro Photon Devices (MPD) have a very similar instrument response. Both of these devices have a similar structure but the MPD detector was grown on an all-silicon substrate without a cavity.

The rapid development of single-photon superconducting nanowire detectors (SSPD) in recent years has seen them being used in many quantum information applications [55],

[56]. These detectors are based around a thin, narrow strip of a superconducting material such as niobium nitride which is biased at close to the critical current while cooled to a temperature of 3 K; a temperature which is below the superconducting transition temperature. An incident photon creates a resistive hotspot as the current density in parts of the nanowire exceeds the critical level, which leads to a readily detectable current pulse. The thin junction Si-SPADs and the SSPD exhibit comparable FWHM timing jitters but unlike Si-SPADS, SSPDs have an approximately Gaussian temporal response, as can be seen in Figure 4.28. An SSPD can be operated at a number of different bias currents. As the bias current is increased the detection efficiency increases but at the expense of a higher dark count rate (DCR). The SSPDs used in this chapter had a detection efficiency of ~10% for light at a wavelength of 850 nm and a DCR level of ~10 counts per second. The benefit of using SSPDs has already been demonstrated at GHz clock rates in various QKD demonstrations at wavelengths of 1550 nm [56] and full field-tests on installed optical fibre [57].

Type	Detector	Dark Count Rate (per second)	Detection Efficiency (%)	FWHM (ps)	FW10%M (ps)	FW1%M (ps)	After pulsing probability
Thick-Junction Si-SPAD	Perkin Elmer	198	42	432	837	1473	0.5%
Thin Junction Si-SPAD	MPD	200	8.4	71	276	898	3%
	IDQ	15	1.6	63	193	1245	3%
	Resonant Cavity	21	18	74	271	913	2%
NbN SSPD Nanowire	SSPD	10	10	62	120	196	-

Table 4.1. The characteristic parameters of the specific detectors when used at a wavelength of 850 nm in the QKD system.

The QKD system was operated using a 180 µm active area diameter PerkinElmer SPCM AQR 12 thick junction Si-SPAD [58], a 20 µm active area diameter thin junction MPD PDM CCTC Si-SPAD [59], a 50 µm active area diameter IDQ id100-MMF50 thin junction CMOS Si-SPAD [60], an experimental 20 µm diameter active area resonant cavity thin junction Si-SPAD [54] and a niobium nitride (NbN) nanowire meander line superconducting single-photon detector (SSPD) with a meander area of 20

μm by 20 μm and a fill factor of 50% [61]. The semiconductor detectors were peltier cooled to an operating temperature in the range ~230 K to ~260 K while the SSPD operated at a temperature of 3 K in a closed-cycle refrigerator [62].

4.2.1 Theoretical model

A theoretical model of the system was developed to predict the QBER, raw photon flux recorded by Bob (raw bit-rate, RBR), the time and basis set sifted photon flux (sifted bit-rate, SBR) and final key generation rate. Although applied specifically to the experimental QKD system described in this chapter, this model can be adapted for use with other QKD systems.

The raw bit rate (R_{Raw}) can be calculated from the clock frequency (ν), the mean photon number per pulse (μ), the length of the fibre (L_{Fibre}), the per unit attenuation of the fibre ($\alpha_{Fibre} = 0.603$ at a wavelength of 850 nm), the transmission coefficient of Bob ($\alpha_{Bob} = 0.22$), the detection efficiency of the single-photon detector ($\alpha_{Detection}$) and the dark count rate of the detector (R_{Dark}):

$$R_{Raw} = (\nu \cdot \mu) \cdot \left((\alpha_{Fibre})^{L_{Fibre}} \cdot \alpha_{Detection} \right) + R_{Dark} \qquad \text{Equation (4.11)}$$

This calculation can be adapted for a system employing decoy states by replacing the constant μ term with a term which describes the variance in the mean photon number. The sifted bit rate (SBR) after time filtering and a random basis set choice ($R_{Sifted}(\Delta T)$) is calculated as

$$R_{Sifted}(\Delta T) = \alpha_{Protocol} \cdot R_{Raw} \cdot I_{System}(\Delta T) \qquad \text{Equation (4.12)}$$

where α_{Protocol} is the protocol loss (which is equal to ½ for the BB84 protocol) and ΔT is the duration of the gate used for temporal filtering. $I_{System}(\Delta T)$ is the fraction of counts that are retained after temporal filtering, which depends on both the duration of the filtering gate and the system detector response function. $I_{System}(\Delta T)$ was modelled from an instrument response of the laser output as recorded by the detector and time-stamping electronics. The experimental system operates at a clock rate of 1 GHz, meaning that for the Si-SPAD detectors there is still a significant degree of temporal intersymbol interference. This is modelled by constructing a temporal probability distribution function ($P_{Arrival}$) for the incoming photons based on the instrument response of the system for a particular detector and the four possible paths which a photon may take through the QKD system. In the phase-basis set system described here

a photon can arrive at the detector having taken one of four possible paths, the short arm in Alice and the short arm in Bob, the delay arm in Alice and the delay arm in Bob, the short arm in Alice and the delay arm in Bob or the delay arm in Alice and the short arm in Bob. The first two possible paths do not experience interference and do not contribute to the secure key and are time-gated out of the measurement analysis. However, the diffusion tails on the temporal response of the Si-SPAD detectors may cause photons which have taken these non-interfering paths to be detected during the gate assigned to the following interfering path. The time delay between the short and delayed paths in Alice and Bob is set to be 500 ps so that the non-interfering pulses are equally time spaced from the preceding and following interfering pulses. This means that over a periodic signal, the pulses from the short in Alice and delay in Bob path are superimposed on those from the delay in Alice and short in Bob path. The maximum clock rate of the QKD system is limited by temporal intersymbol interference resulting from the diffusion tails of photons following the non-interfering paths. QKD systems which operate using different techniques for basis set measurements (e.g. those not using matched interferometer delays or those using polarisation basis sets) will have a different temporal probability distribution which can be modelled in a similar way.

Figure 4.29 shows $P_{Arrival}$ for an MPD detector and can be considered a probability distribution of the possible times at which a photon from a single pulse may reach the detector. Therefore

$$I_{System}(\Delta T) = \frac{1}{\int_0^{2\frac{1}{\nu}} P_{Arrival}\,dt} \cdot \int_{t_{\max}-\Delta T/2}^{t_{\max}+\Delta T/2} P_{Arrival}\,dt \qquad \text{Equation (4.13)}$$

where $t_{\max}$ is as defined in Figure 4.29 and $P_{Arrival}$ is defined for a duration of $2/\nu$. The probability distribution $P_{Arrival}$ is formed using a system instrument response, such as those shown in Figure 4.28. To reduce the effects of noise on the signal, the instrument response was modelled as $D_{Response}$ using a piecewise exponential representation[63] whose form is given by Equation (4.14).

$$D_{\text{Response}} = \begin{cases} e^{\frac{-(t-t_0)t}{2\sigma^2}}, & t < t_1 \\ C_1 \cdot e^{\frac{-t}{\tau_1}}, & t_1 \le t \le t_2 \\ C_2 \cdot e^{\frac{-t}{\tau_2}}, & t_2 \le t \le t_3 \\ C_3 \cdot e^{\frac{-t}{\tau_3}}, & t_3 \le t \le t_4 \\ C_4 \cdot e^{\frac{-t}{\tau_4}}, & t \ge t_4 \end{cases} \qquad \text{Equation (4.14)}$$

where σ^2 is the variance of the Gaussian region, C_1, C_2, C_3 and C_4 are multiplicative constants, t_0 is the time of the maximum count return in the peak and t_0, t_1 ,t_2, t_3 and t_4 are the points at which the transitions between functions occur. These values are calculated using an iterative Levenberg–Marquardt algorithm [64]. The SSPD was modelled using the Gaussian term alone, with no need for the exponentials which define the diffusion tail. The fits resulting from this model are shown by the dashed lines in Figure 4.28 and the fitting parameters are shown in Table 4.2.

The parameters used for the piecewise exponential fits on the instrument responses are listed in Table 4.2. The parameter t_0 defines the peak position of the instrument response so the transition points are quoted in Table 4.2 with respect to this parameter. To construct $P_{Arrival}$, the piecewise fit $D_{Response}$ was plotted at each of the possible time-periods at which a photon could arrive at a detector with the amplitude dependent on the relative loss of the path taken, as shown in Figure 4.29 for the MPD Si-SPAD (blue). The simulated trace from an SSPD (red) is shown for illustrative purposes. $P_{Arrival}$ then is the summation of the different overlapping $D_{Response}$ functions for a particular detector, as indicated by the grey dashed line in Figure 4.29 for the MPD Si-SPAD. $P_{Arrival}$ is periodic and detectors tails exiting the graph at $2/\nu$ re-enter at zero time. The function $P_{Arrival}$ will change for other QKD systems but using the principle described here allows other systems to be modelled in a similar fashion treating the arrival time of the photon as a probabilistic event.

	Detector	$t_1 - t_0$ (ps)	$t_2 - t_0$ (ps)	$t_3 - t_0$ (ps)	$t_4 - t_0$ (ps)	τ_1 (ps)	τ_2 (ps)	τ_3 (ps)	τ_4 (ps)	σ (ps)
Thick Junction Si-SPAD	PerkinElmer	240	350	636.5	940	151.7	144.15	270.54	603.7	125
Thin Junction Si-SPAD	MPD	36.3	56.3	104.3	626.3	42	83.75	225.64	291.6	21
	IDQ	37	98	668	1070	33	413	1076	1296	20
	Resonant Cavity	20	70	120	420	39.63	118.6	270.6	347.9	17
NbN Superconducting Nanowire	SSPD	—	—	—	—	—	—	—	—	69.5

Type	Detector	C_1	C_2	C_3	C_4	Coefficient of Determination r^2	Goodness of Fit χ^2
Thick Junction Si-SPAD	PerkinElmer	1.5×10^{3}	2.5×10^{3}	13	0.25	0.997	1.00
Thin Junction Si-SPAD	MPD	2.7×10^{10}	0.91×10^{5}	23	4.5	0.998	1.00
	IDQ	1.4×10^{13}	0.85	0.07	0.05	0.946	1.00
	Resonant Cavity	3×10^{8}	2×10^{2}	2.82	1.1	0.985	1.00
NbN Superconducting Nanowire	SSPD	—	—	—	—	1.00	1.00

Table 4.2. The parameters used in the piecewise exponential fits to the instrument responses shown in Figure 4.28 and the coefficient of determination and goodness of fit of the resulting fits.

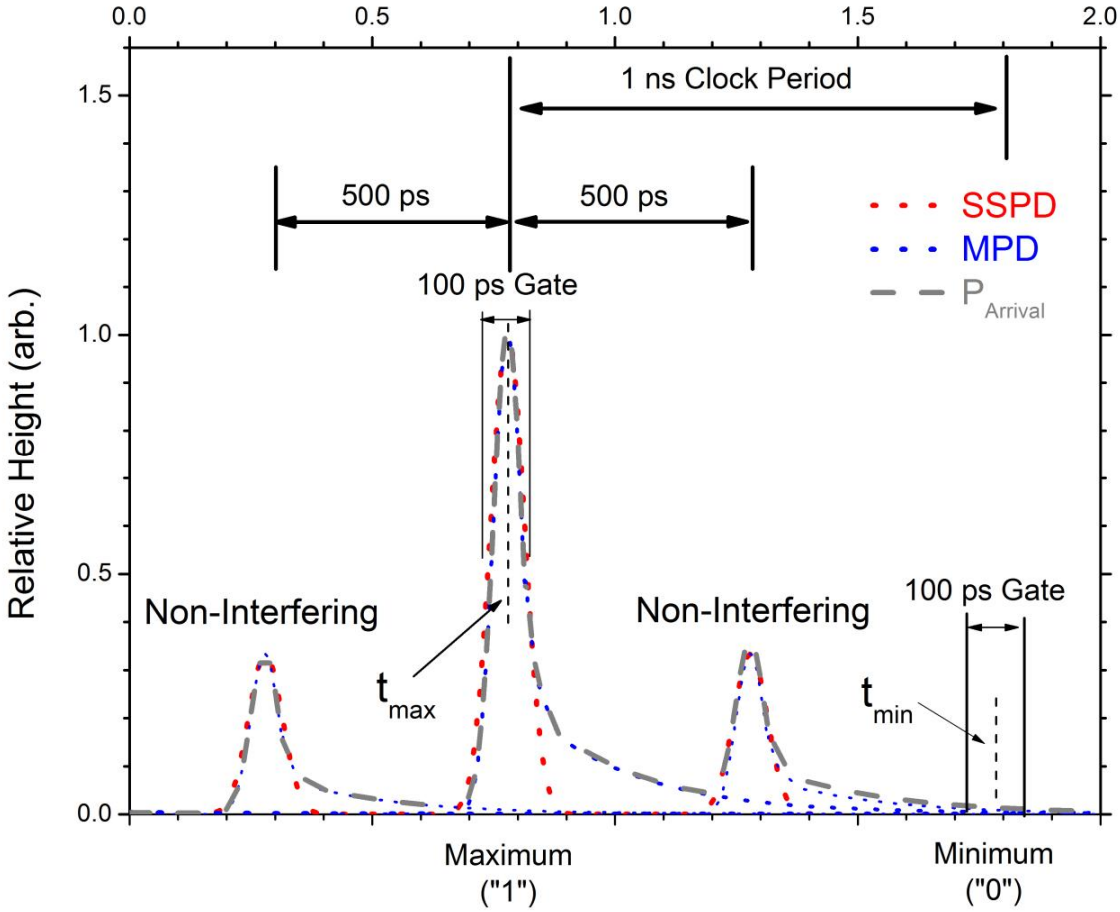

Figure 4.29. The probability distribution for the theoretical model of the expected arrival time of the photon. The red curves are the results obtained by simulating a histogram of a 1010 repetitive sequence on one SSPD. The blue curves are the individual detector response for each peak simulated using an MPD detector. The grey curve is the summation of the individual blue MPD detector curves, indicating the intersymbol interference. All curves are created using the piecewise exponential model. The probability distribution is periodic and curves which have not reached zero by the maximum time will re-enter the graph at minimum time and continue to decay until they reach zero. This probability distribution can be adapted for any QKD system by considering the shape of the entire system response over one clock period.

The definition of $P_{Arrival}$ given in Figure 4.29 considers perfect interferometric visibility and therefore perfect destructive interference at time $t_{\min}$. Any counts observed in the temporal gate between $t_{\min} - \Delta T/2$ and $t_{\min} + \Delta T/2$ are, provided ΔT is short relative to the clock period, caused by intersymbol interference.

Calculation of a final secure bit rate requires calculation of the QBER. In a generic QKD system, the QBER can be expressed as containing contributions from the decoding of the quantum states (measurement at Bob), errors in the encoding of the states at Alice, the dark counts of the detector and the timing jitter of the complete system:

$$QBER_{total} = QBER_{Decoding} + QBER_{encoding} + QBER_{Dark} + QBER_{Jitter} \quad \text{Equation (4.15)}$$

Each term can be calculated once the characteristic parameters of the system are known which allows the final QBER to be calculated. The term $QBER_{Decoding}$ is caused by the classical visibility of the interferometers which make up Alice and Bob and can be expressed as [65]:

$$QBER_{Decoding} = \frac{1 - \vartheta_{Visibility}}{2} \quad \text{Equation (4.16)}$$

where $\vartheta_{visibility}$ is the classical visibility expressed as a fraction. This was measured to be 0.98, which indicates that the contribution to the QBER from the visibility is 1%. In a fully optimised system based on double asymmetric Mach-Zehnder interferometers it is possible to reduce this contribution to less than 0.1% [66]. This may be achieved using a narrower linewidth source such as a distributed feedback laser (DFB) which can typically have a linewidth in the MHz region [67]. In a polarisation basis set QKD system, like the one described in Chapter 3, this term can be calculated from the extinction ratio of Bob's polarisation analysers. The term $QBER_{Encoding}$ defines the contribution to the QBER caused by errors in Alice's encoding of the quantum states on the photons. In this system it is due to phase jitter in Alice's modulator which can be modelled as [68]:

$$QBER_{Encoding} = \frac{1}{\Delta\phi} \int_{-\frac{\Delta\phi}{2}}^{+\frac{\Delta\phi}{2}} \frac{1 - \cos\phi}{2} d\phi \quad \text{Equation (4.17)}$$

where $\Delta\phi$ is the variation in phase caused by the modulator. The driving electronics for the phase modulator, which include PPG jitter and amplifier jitter, were found to have an amplitude jitter of 354 mV, corresponding to a $\Delta\phi$ of 0.69 rad and a contribution to the QBER from phase jitter of 1%. In a polarisation basis set system this term can be calculated from the polarisation jitter in Alice's polarisation modulator if an

active scheme is used, or the extinction ratio of her polarisers if a passive scheme is used.

The contribution to the total QBER caused by the dark count rate of the detector becomes more significant at longer transmission distances when the photon flux reaching Bob is greatly reduced. This contribution can be calculated via:

$$QBER_{Dark} = \frac{\frac{1}{2} \cdot \alpha_{\text{Protocol}} \cdot \upsilon \cdot \Delta T \cdot R_{Dark}}{R_{Sifted}\left(\Delta T\right)} \qquad \text{Equation (4.18)}$$

When the dark count events are histogrammed the events are randomly and evenly distributed across the entire histogram range.

Calculation of $QBER_{Jitter}$ requires the model developed in Figure 4.29. The value for $QBER_{Jitter}$ is given by the ratio of the probability of finding a photon in the gate around the minimum (destructive interference) position to the sum of this probability of finding a photon in maximum (constructive interference) and minimum position (i.e. total number of photons in the timing gates).

$$QBER_{Jitter} = \frac{\int_{t_{\min}-\frac{\Delta T}{2}}^{t_{\min}+\frac{\Delta T}{2}} P_{Arrival}\,dt}{\int_{t_{\min}-\frac{\Delta T}{2}}^{t_{\min}+\frac{\Delta T}{2}} P_{Arrival}\,dt + \int_{t_{\max}-\frac{\Delta T}{2}}^{t_{\max}+\frac{\Delta T}{2}} P_{Arrival}\,dt} \qquad \text{Equation (4.19)}$$

The theoretical model predicts the best QBER that may be obtained from an experimental system and does not take into account time-varying changes in the alignment which can lead to fluctuations in the observed values of QBER. These fluctuations are stochastic in nature and the precise QBER at a particular time cannot be determined from the model. An upper bound on the QBER will occur when the alignment drifts to the point where the phase states are out of phase.

Calculation of the final secure bit rate must take into account the error correction which will be required to generate a final, secure key [69]. The exact fraction of sifted bits used in the generation of the secure key depends on the algorithm employed, but all commonly employed QKD error correction algorithms [70] and security analysis have a

strong logarithmic dependence on QBER. From work published by Gottesman, Lo, Lütkenhaus and Preskill (GLLP) the net bit rate $R_{Net}(\Delta T)$ can be calculated as:

$$R_{net}(\Delta T) = \left((1-\Delta) - f_p \cdot H_2(QBER_{Total}) - f_p \cdot (1-\Delta) \cdot H_2\left(\frac{QBER_{Total}}{1-\Delta} \right) \right) \cdot R_{Sifted}(\Delta T)$$

Equation (4.20)

where $H_2(x)$ is the binary entropy function [71] given by

$$H_2(x) = -x \cdot \log_2(x) - (1-x) \cdot \log_2(1-x) \qquad \text{Equation (4.21)}$$

f_p is the efficiency of the error correction protocol relative to the Shannon limit (for the Cascade error correction protocol [69] f_p has a value of 1.16) and Δ is the fraction of pulses intercepted by an eavesdropper. In the analysis presented here this is given by:

$$\Delta \approx \frac{\mu^2}{2} \qquad \text{Equation (4.22)}$$

for a weak coherent pulsed source. This analysis does not consider the photon number splitting attack which for a weak coherent source the μ value must be reduced according to the channel loss. For a full analysis Equation (4.22) must be modified to become

$$\Delta = \frac{p_M}{p_D} \qquad \text{Equation (4.23)}$$

where p_M is the probability of Alice emitting a multiphoton pulse and p_D is the fraction of the pulses which has been detected at Bob. The value p_D takes into account the loss of the quantum channel in addition to inefficiencies in Bob's detectors. In an ideal photon number splitting attack Eve replaces the transmission link with a lossless channel and only allows multiphoton pulses to be sent to Bob, after keeping one photon for herself. Figure 4.30 shows the key generation rate when a full GLLP security analysis is applied for QKD systems operating at wavelengths of 1550, 1310 and 850 nm using the same detection efficiency. The higher transmission loss at a wavelength of 850 nm in telecommunication fibre limits its range to about 2 km while at 1550 nm that distance can be extended to just over 30 km.

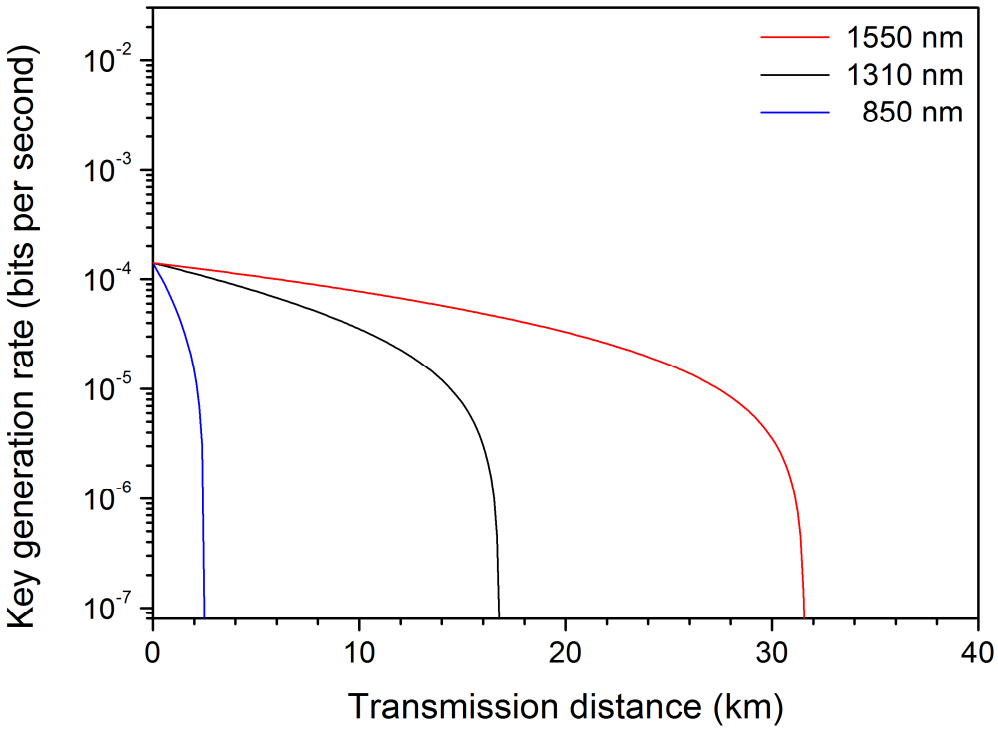

Figure 4.30. The key generation is shown for a wavelength of 1550 nm, 1310 nm and 850 nm using a full GLLP analysis. The attenuation per km of telecoms fibre at wavelengths of 1550, 1310 and 850 nm are 0.22, 0.35 and 2.2 dB/km respectively. The values used in the model have been taken from Gobby et al.'s system operating at a wavelength of 1550 nm[66]. For the purposes of comparing the key generation rate at the different wavelengths the same detector efficiency is used and QBER values. At 1550 nm key generation is successful up to about 30 km, however the higher attenuation of optical fibres at 850 nm means that key generation using the full GLLP analysis is only successful about up to two kilometres.

4.2.2 GHz phase basis set QKD results

The performance of the QKD system described can be tested with a variety of fibre connectorised detectors as required. This allows a quantitative comparison of how the characteristic of a given detector can affect a QKD system. Figure 4.31 and Figure 4.32 show the lowest experimentally recorded quantum bit error rate (QBER) and corresponding net bit rate (NBR) for the five different detectors employed. The dashed lines in both figures show the results of the theoretical model when applied to the five detectors and Table 4.2 quantifies the quality of the theory model.

Table 4.3 shows the contributions to the QBER due to detector timing jitter. Due to the availability of optical fibre, a calibrated optical attenuator was used to simulate real fibre.

The shape of the QBER graph is primarily determined by the timing jitter profile, dark count rate and the detection efficiency of the detector. The thick junction PerkinElmer Si-SPAD exhibits a baseline QBER of about 7.2% which is higher than those observed when using the thin junction SPADs. The instrument response of the thick junction Si-SPAD shows a FWHM of 432 ps in comparison to ~67 ps for the thin junction Si-SPADs. Consequently there is a higher possibility of photons being time tagged in an incorrect window thereby increasing the QBER. If the instrument response is considered as a probability distribution of arrival time for the photon then it can be seen that a longer FWHM timing jitter will have a greater effect on the QBER than a longer FW10%M. Using detectors with comparable FWHM timing jitters, a longer FW10%M will lead to an increase in QBER. The higher baseline QBER obtained using the IDQ Si-SPAD in comparison to the MPD Si-SPAD, which both have a similar FWHM is partially due to the longer FW10%M and partially due to the much lower detection efficiency of the IDQ detector of 1.6% compared to the MPD detector efficiency of 8.4%. Although they both have similar FWHM timing jitter, the resonant cavity Si-SPAD exhibits a baseline QBER of 4% while the SSPD exhibits a baseline QBER of 2%. This is mainly due to the tail present in the temporal response of the resonant cavity Si-SPAD which is completely absent in the SSPD response.

Following basis set reconciliation defined in the BB84 protocol to produce the sifted key, the detected photon events are temporally filtered to reduce the effect of dark counts using a gate of 100 ps duration centered on the most probable detection time. Figure 4.31 shows the variation in the NBR with transmission distance for each of the detectors used. The superior timing resolution of the SSPD of 196 ps FW1%M compared to 913 ps FW1%M for the resonant cavity Si-SPAD means that the NBR for the SSPD was larger even though its detection efficiency was 10% compared to 18% for the resonant cavity device. As a consequence of the lower overall QBER values obtained for the SSPD and the relatively high defection efficiency and good timing resolution for the resonant cavity Si-SPAD, these detectors gave the highest NBRs compared to the other detectors.

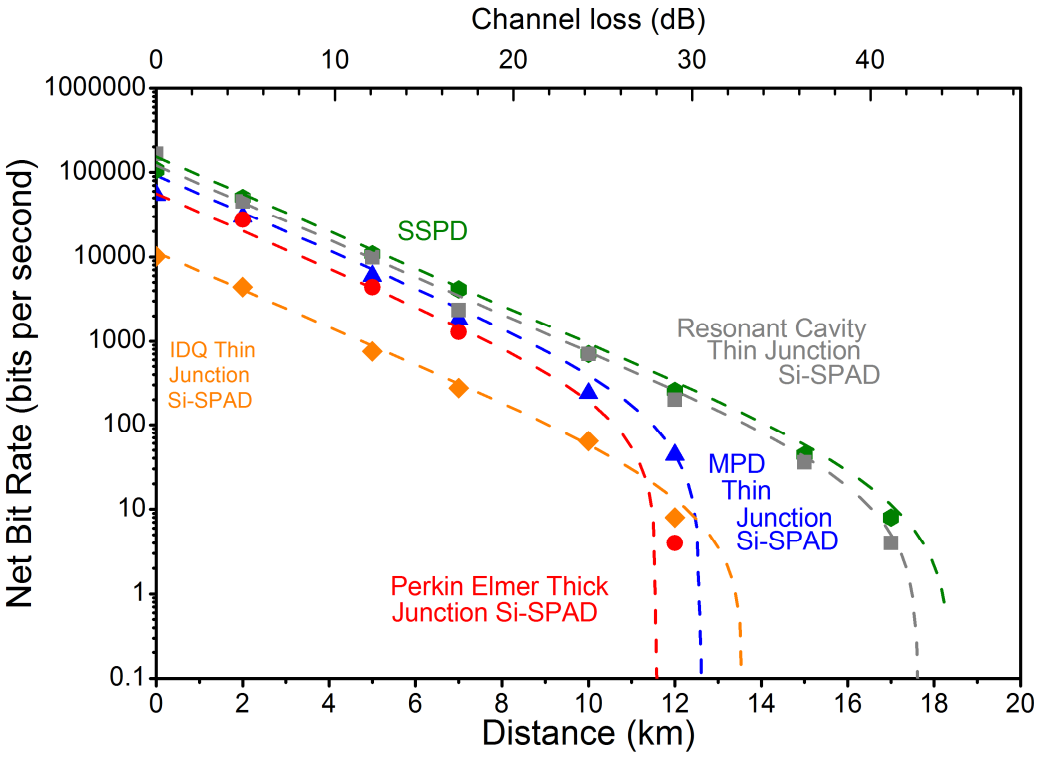

Figure 4.31. The highest bit rate obtained against distance for the 5 detectors used. The dashed lines show the predictions made by the theoretical model.

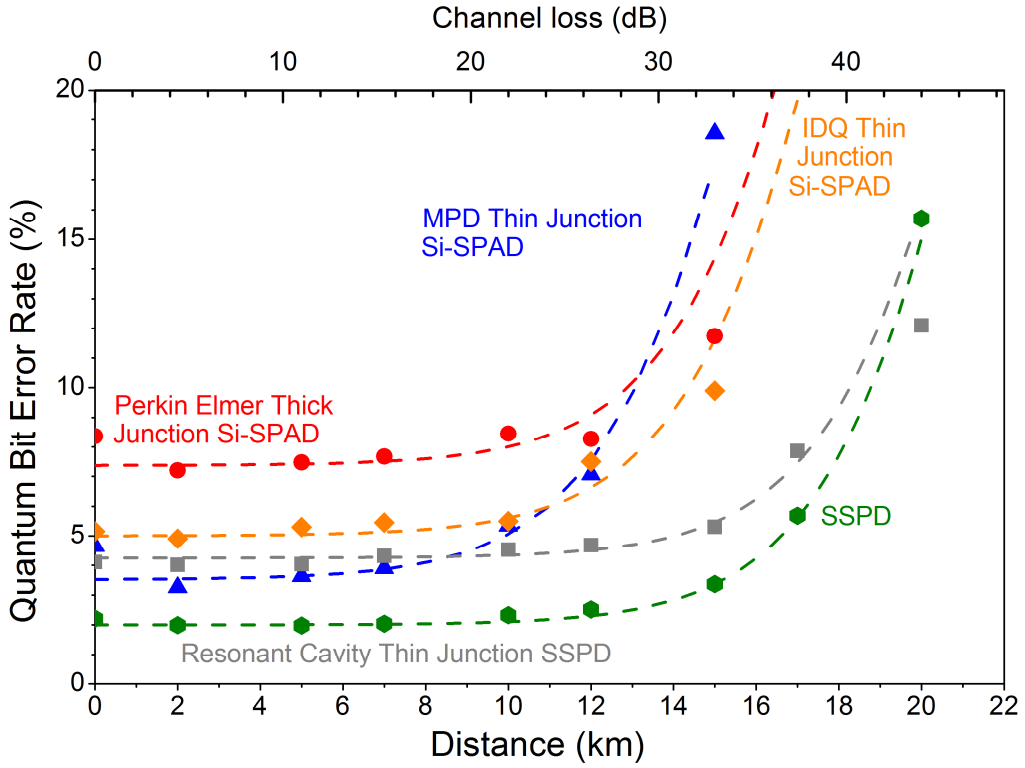

Figure 4.32. The lowest QBER obtained against distance for the 5 detectors. The dashed lines show the predictions made by the theoretical model.

Type	Detector	$QBER_{Jitter}$ (%)
Thick Junction Si-SPAD	PerkinElmer	6.0
Thin Junction Si-SPAD	MPD	2.9
	IDQ	2.5
	Resonant Cavity	3.3
NbN Superconducting Nanowire	SSPD	0.0

Table 4.3. The quantum bit error rate due to detector timing jitter ($QBER_{Jitter}$) for the detectors presented in this Chapter.

4.2.3 Effect of temporal gate on the QBER and NBR

To minimise the effects of dark counts in the system a temporal window is opened on the expected time of arrival of a photon. The duration of this window can affect the QBER and NBR from the system. The PerkinElmer thick junction Si-SPAD has a FWHM timing jitter of 432 ps which exceeds the ΔT temporal gate duration of 100 ps and results in some temporal filtering of the raw detector events. Figure 4.33 shows the effect of varying the gate duration on both the QBER and NBR.

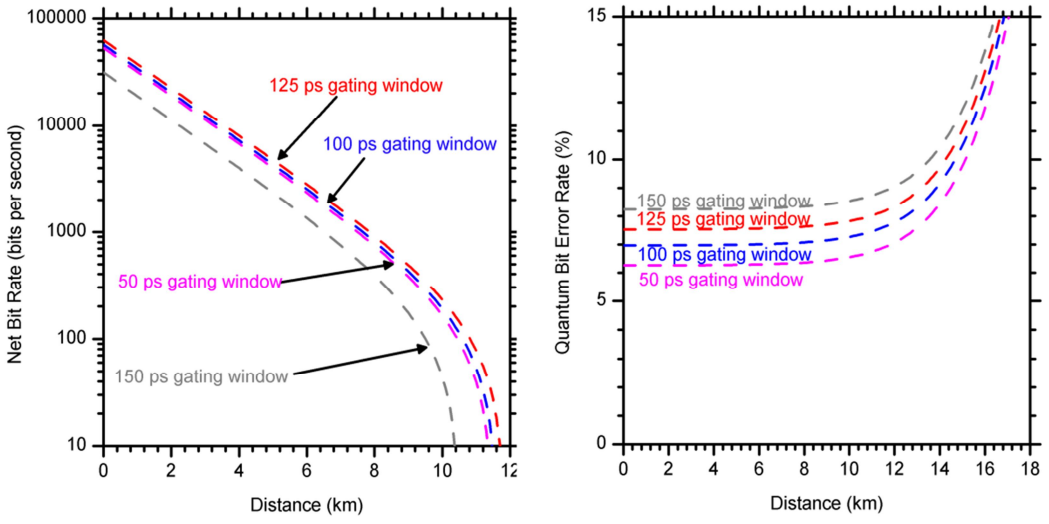

Figure 4.33. The effect of varying ΔT, the gate duration, on the PerkinElmer thick-junction Si-SPAD.

Increasing the gate duration increases the counts within both the $t_{min} \pm \Delta T/2$ and $t_{max} \pm \Delta T/2$ temporal windows. Increasing the duration of ΔT increases the effect of intersymbol interference which leads to increase in the baseline QBER. In the case of the NBR an increase in the temporal window increases the counts included in the $t_{min} \pm \Delta T/2$ and $t_{max} \pm \Delta T/2$ temporal windows. However an indefinite increase in ΔT does not necessarily lead to ever increasing NBR values as the QBER rises with longer duration ΔT, as observed in the case of the 150 ps temporal window where the reduction in the NBR is due to the higher QBER for this ΔT.

4.2.4 Long term stability results

To demonstrate the long term stability of the QKD system, it was left to run continuously for a period of 24 hours fully autonomously and without operator intervention using the resonant cavity thin junction Si-SPAD and SSPD detectors. During this period, the bit rates and QBER were automatically recorded and are shown in Figure 4.34 and Figure 4.35 for the resonant cavity device. A fixed fibre distance of 2 km was used throughout these measurements. The system was operated in enclosed aluminium boxes which help to maintain the stability of the interferometers in a laboratory. Air conditioning maintained the temperature of the laboratory to within ±2.5 °C. The mean NBR was 7.75 kbits s^{-1} (excluding the tuning phases), the mean QBER was 6.9% and the system was transmitting key for 68% of the duration of the experiment. When the SSPD was operated the mean NBR was 17.6 kbits s^{-1} (excluding the tuning phases), the mean QBER was 3.49% and the system was transmitting key for 82% of the duration of the experiment. The insert in Figure 4.34 shows the voltage applied to the piezo electric actuator located in the vernier mechanism in the airgap in Bob over the first 6 hours operation. Custom tuning software adjusts this voltage to compensate for path length drift due to environmental fluctuations. The SSPD gave superior average NBR and lower average QBER values over the resonant cavity device. Although part of this is explained by the lower QBER values resulting from the superior timing resolution of the SSPD, part of it is due to the time duration in which the system was transmitting key. The run with the SSPD was stable for 82% of the time but this is in no way dependent on the detector choice but on the random variations in temperature and air currents in the laboratory from day to day which can destabilise the interferometers.

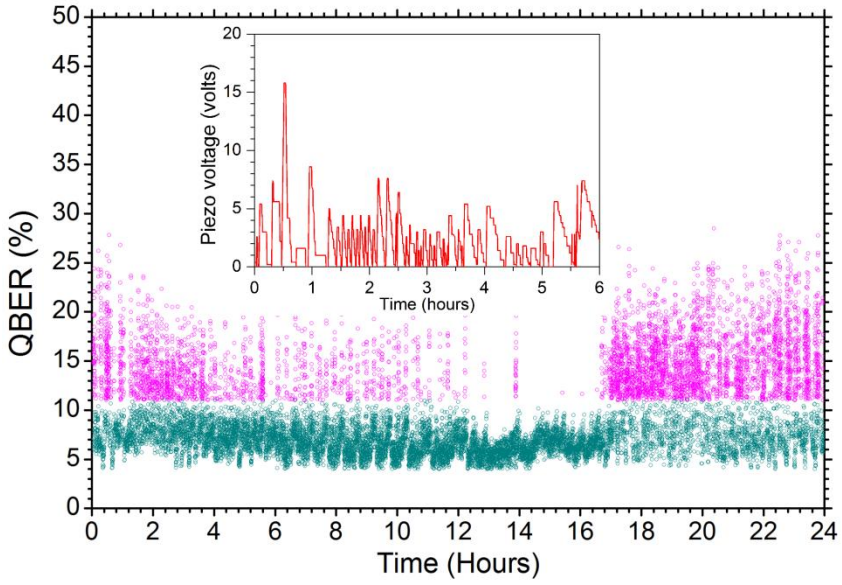

Figure 4.34. The QBER against time for 24 hour fully automated operation of the environmentally robust QKD system using the resonant cavity thin junction Si-SPAD. When the QBER exceeded a threshold value, automatic tuning was initiated, as indicated by the red points in the top graph, and key generation was temporarily halted as the air gaps were adjusted to minimise the QBER. The insert shows the applied voltage to the piezoelectric controlled adjustable air gap for tuning. The flat parts of the trace represent times when the interferometers are stable and the applied voltage does not need to vary. To go from destructive interference to constructive interference required the voltage applied to the piezo actuator to change by about 2.8 volts. The average voltage change that needed to be applied to tune the interferometer was 0.24 volts.

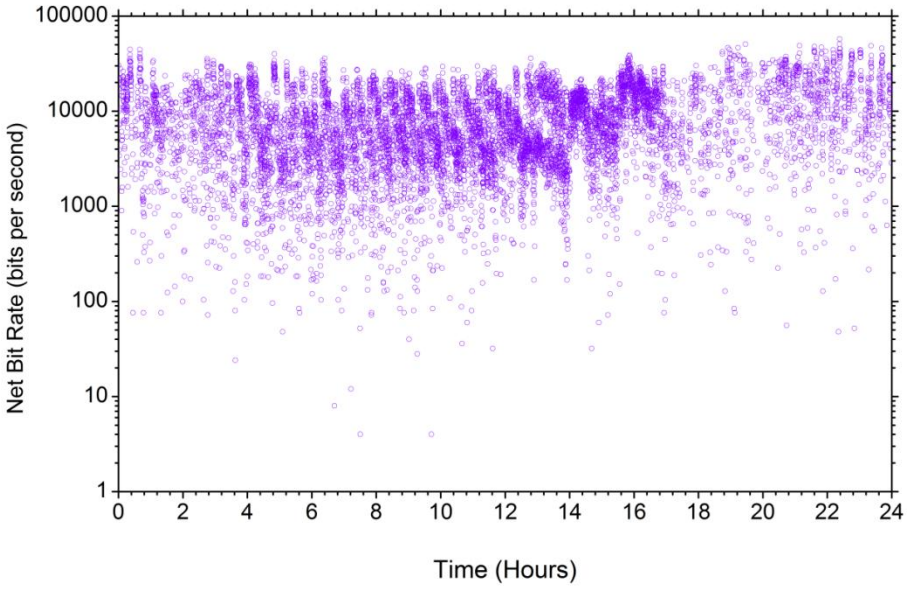

Figure 4.35. The NBR against time for 24 h fully automated operation of the environmentally robust QKD system using the resonant cavity thin junction Si-SPAD.

4.2.5 Predictions of future system performance with detector improvements

Since the first observations of single-photon pulses in avalanche photodiode biased above breakdown in the 1970s [72] there has been rapid progress over the years. Efforts have been made at understanding how the device geometry and the readout electronics can affect the overall performance of the detector with the aim of making improvements. The long tail in the instrumental response of the Si-SPADs, due to minority carriers drifting from the neutral region into the active region can be reduced or eliminated by altering the detector structure. Double epitaxial structures like the one shown in Figure 4.36 have been grown in which the active junction is built in the p-epilayer and the substrate/epistrate np junction is at zero or reverse bias. Electrons which have been photo-generated in the substrate are not able to reach the epilayer. The substrate/epistrate junctions are in competition with the active junction in collecting the electrons generated in the neutral p-epilayer which helps reduce the diffusion tail effect in the instrumental response function.

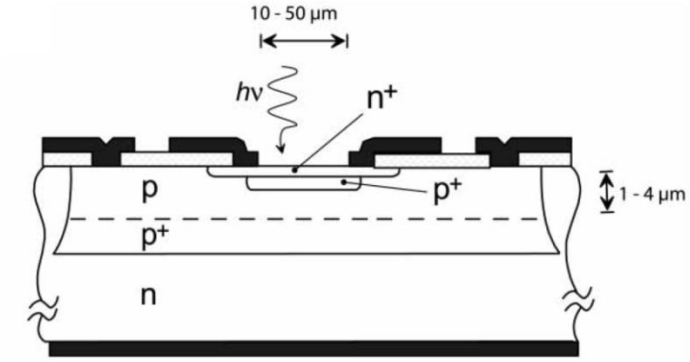

Figure 4.36. Schematic cross section of a planar epitaxial device developed by Cova et al. [73].

The FWHM timing jitter of a PerkinElmer thick junction Si-SPAD can be reduced by modifying the pulse readout electronics within the detector module which makes it possible to extract the avalanche current from the detector without affecting the initial rise time [74]. This modified circuit reduces the FWHM of the detector without affecting the dark count rate or detection efficiency. The shortest unmodified PerkinElmer Si-SPAD FWHM reported in the literature, was by Restelli *et al.* in a previous free-space GHz clock rate QKD system demonstration, was 350 ps, which decreased to 200 ps after circuit modification [75]. This modified detector had similar detection efficiency to the thick-junction detector used in these experiments. With these improvements in detector timing resolution and future possible developments, a prediction of how the QKD system would perform in this scenario has been made.

The theoretical model was used to calculate the total QBER for the detector used by Restelli *et al.* in its initial and modified state if it had been possible to use it in the QKD system described in this chapter. In modelling the QKD system performance it was assumed that the detector of Restelli *et al.* exhibited the same DCR and FW10%M and FW1%M as the thick junction Si-SPAD used experimentally in this chapter. A detector with a FWHM jitter of 390 ps was also modelled, which was chosen as halfway between the FWHM of the unmodified PerkinElmer Si-SPAD used experimentally and the unmodified PerkinElmer Si-SPAD of Restelli *et al.* The theoretically predicted QBER values and NBR are shown in Figure 4.37, along with the experimentally observed QBER for the resonant cavity thin junction Si-SPAD and the SSPD as performance indicators. The FWHM of the unmodified PerkinElmer Si-SPAD used in the QKD system is comparable to the time delay of 500 ps between interfering and non-interfering paths introduced by the path length difference in the interferometers. As the FWHM is reduced, the effect of temporal intersymbol interference is reduced, thus lowering the QBER.

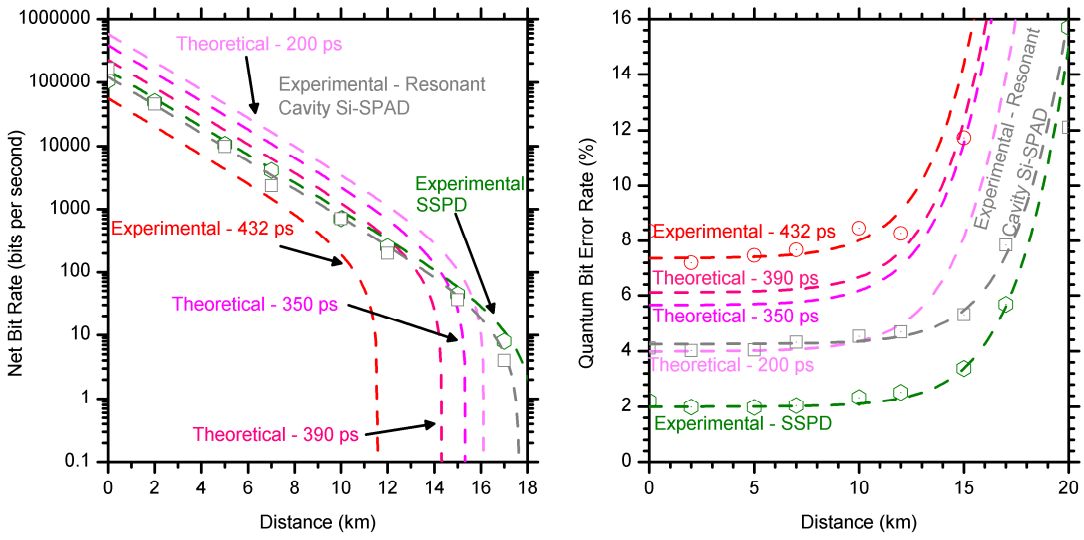

Figure 4.37. Theoretical model results for a PerkinElmer thick junction Si-SPAD with identical efficiency and dark count rate, but with varying FWHM durations of 200ps, 350ps and 390ps. This is compared to the theoretical and experimental results obtained with the detector jitter of FWHM of 432 ps. The FWHM of 200 ps was chosen as it represents the lowest timing jitter of such a thick junction detector in a QKD system found in the literature [76]. The grey dotted line indicates the theoretical fit to the experimental results for the resonant cavity thin junction Si-SPAD and the green dotted line is theoretical fit for the SSPD. Hollow data points represent the experimentally recorded values for the PerkinElmer thick junction Si-SPAD with a FWHM timing jitter of 432 ps, the SSPD and the resonant cavity thin junction Si-SPAD.

The detector temporal response affects the baseline QBER as higher values of the FWHM lead to greater levels of intersymbol interference and a greater contribution to the overall QBER from Equation (4.19). The sifted bit rate (SBR) also increases due to higher probability of photons arriving in the 100 ps time gate. From Equation (4.12) it can be observed that $I_{System}(\Delta T)$ acts as a scaling factor between the raw bit rate and the sifted bit rate and the resultant values

for are shown in Table 4.4. The grey dotted line in Figure 4.37 shows the theoretical fit to the experimental results for the resonant cavity thin junction Si-SPAD and the green dotted line shows the theoretical fit to the experimental results for the SSPD.

Timing Jitter FWHM (ps)	$I_{System}(\Delta T)$	$QBER_{Jitter}$ (%)
432	0.10	6.0
390	0.11	4.6
300	0.12	4.2
250	0.17	2.5

Table 4.4. The effect of altering the FWHM timing jitter of a PerkinElmer thick junction Si-SPAD. $I_{Sytem}(\Delta T)$ is the scaling factor from the raw bit rate and the sifted bit rate, as can be seen from Equation 5.2. The resulting quantum bit error rates (QBERs) are shown in Figure 5. ΔT, the duration of the temporal gate, was 100 ps.

Thin junction Si-SPADs typically exhibit long diffusion tails in the instrument response due to carrier pairs being photo-generated outside the detector depletion region and slowly diffusing into the depletion region [77]. It is possible to reduce the duration of these diffusion tails by altering the microstructure geometry. The piecewise exponential model for the system instrument response presented in Equation (4.14) allows a prediction of how Si-SPADs with different diffusion tails would affect the performance of the QKD system. For comparison purposes, the thick junction Si-SPAD was also subjected to the same modelling approach.

The τ values presented in Table 4.2 were scaled to 90%, 80% and 70% of the original values to simulate shorter decay tails and the resulting QBERs and NBRs are shown in

Figure 4.38 and Figure 4.39 respectively. As the duration of the diffusion tail is decreased, the contribution to the overall QBER from intersymbol interference ($QBER_{Jitter}$ in Equation (4.15)) decreases. This leads to a reduction in the overall modelled QBER and a corresponding increase in the NBR.

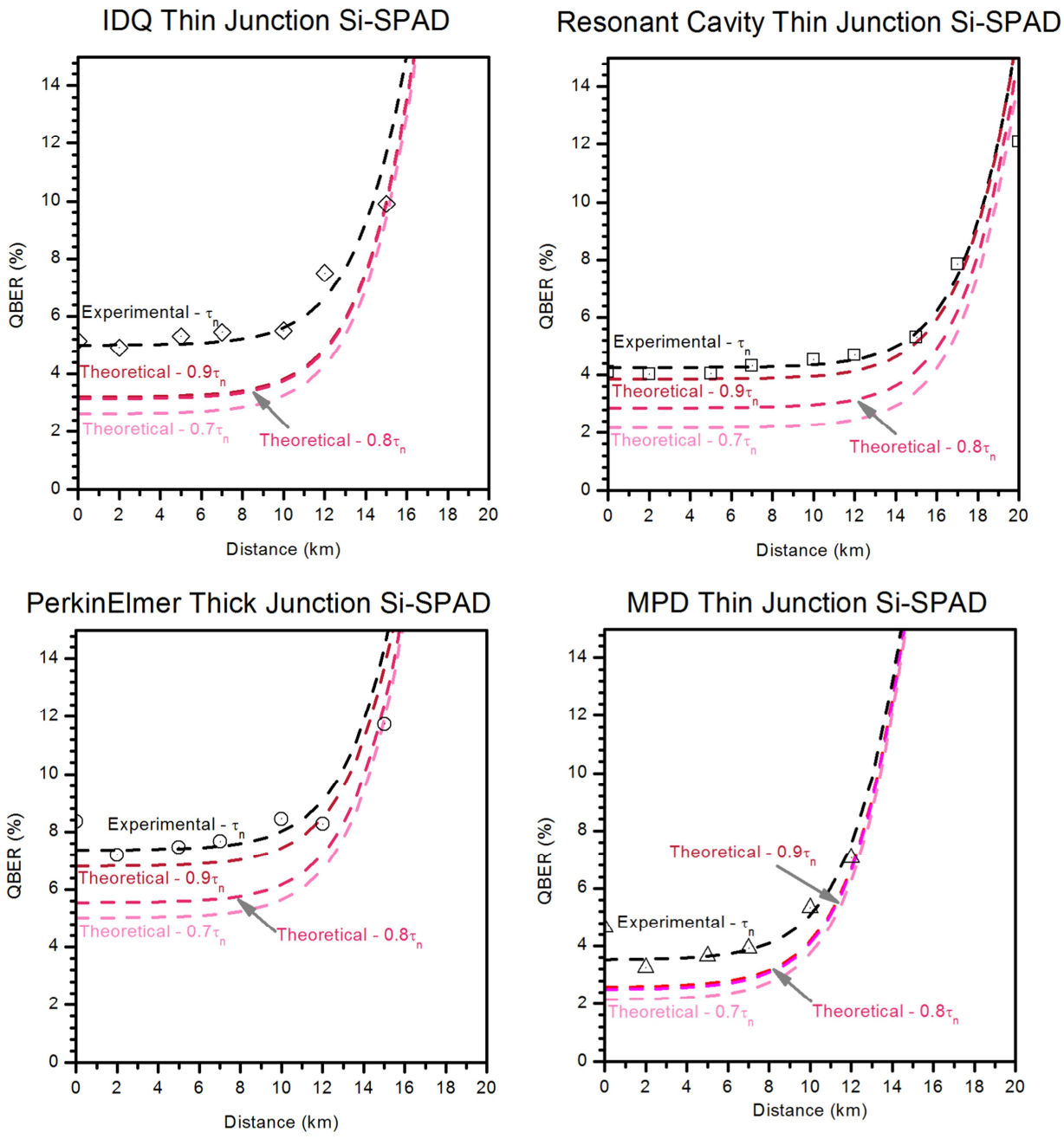

Figure 4.38. Results from the theoretical model showing the effects on the QBER of altering the decay tails of the instrumental responses of the Si-SPADs by changing the τ values in the piecewise exponential fit model of Equation (4.14). The τ values were reduced relative to the values quoted in Table 4.2 as denoted by the scaling factors.

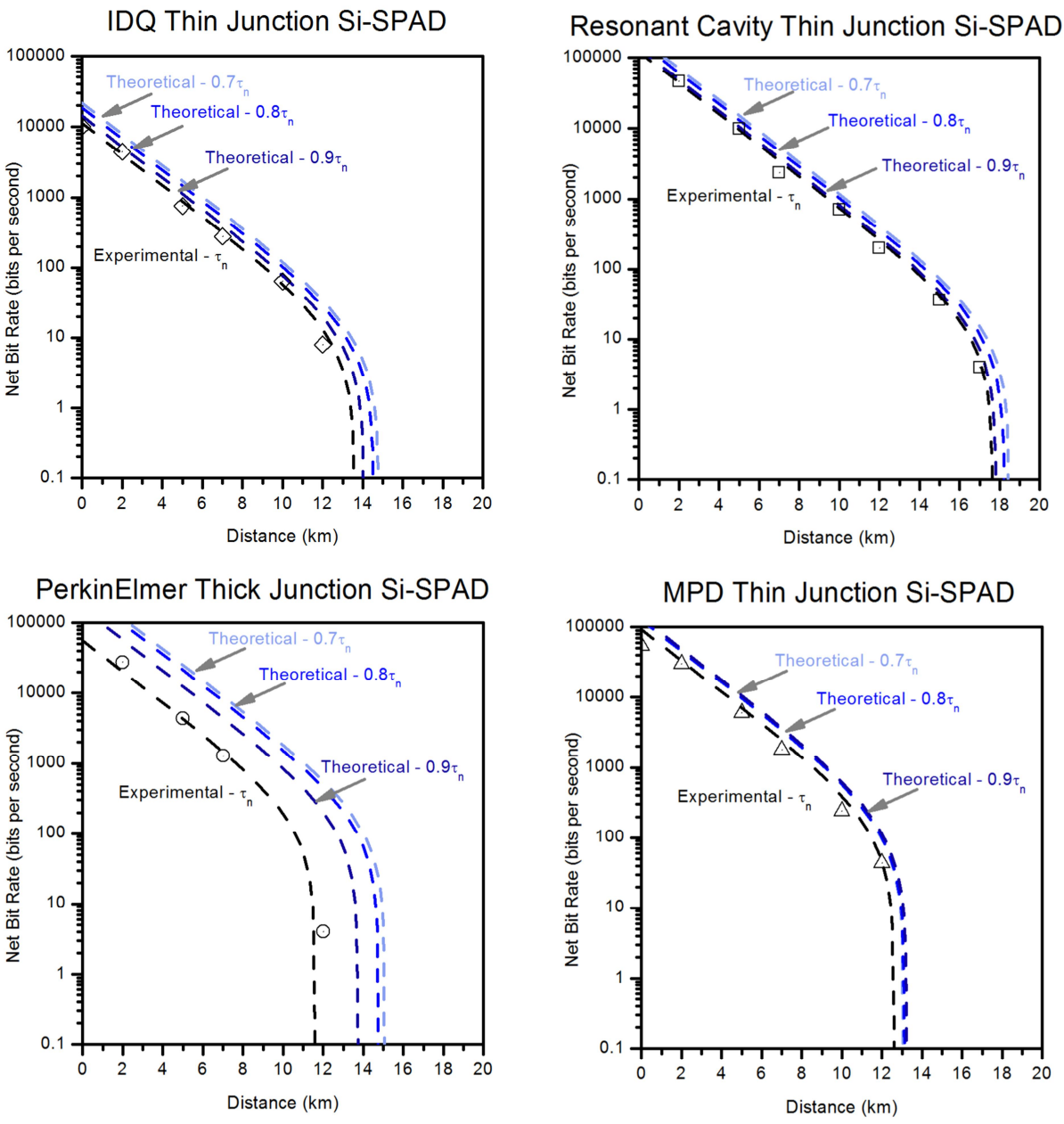

Figure 4.39. Results from the theoretical model showing the effects on the net bit rate (NBR) of altering the decay tails of the instrument responses of the Si-SPADs by changing the τ values in the piecewise exponential fit model of Equation (4.14). The τ values were reduced relative to the values quoted in Table 4.2, as denoted by the scaling factors.

τ Values		100%				90%			
Type	Detector	FWHM (ps)	FW10%M (ps)	FW1%M (ps)	$I_{system}(\Delta T)$	FWHM (ps)	FW10%M (ps)	FW1%M (ps)	$I_{system}(\Delta T)$
Thick Junction Si-SPAD	PerkinElmer	432	837	1473	0.10	424	811	1295	0.10
Thin Junction Si-SPAD	MPD	71	276	898	0.27	68	240	736	0.37
	IDQ	63	193	1245	0.22	63	141	834	0.30
	Resonant Cavity	74	271	913	0.22	59	288	964	0.24

τ Values		80%				70%			
Type	Detector	FWHM (ps)	FW10%M (ps)	FW1%M (ps)		FWHM (ps)	FW10%M (ps)	FW1%M (ps)	$I_{system}(\Delta T)$
Thick Junction Si-SPAD	PerkinElmer	416	772	1222	0.14	415	765	1154	0.1
Thin Junction Si-SPAD	MPD	65	204	646	0.296	65	168	134	0.5430
	IDQ	63	135	552	0.486	63	134	430	0.5
	Resonant Cavity	61	227	815	0.28	71	159	629	0.32

Table 4.5. The effect of altering the τ values in the piecewise exponential fit model of Equation (4.14) on the full-width at half-maximum (FWHM), full-width at 10^{th}-maximum (FW10%M) and full-width at 100^{th}-maximum (FW1%M). $I_{system}(\Delta T)$ is the scaling factor from the raw bit rate and the sifted bit rate, as can be seen from Equation (4.12). ΔT, the duration of the temporal gate, was 100 ps. The resulting NBR and quantum bit error rate (QBER) values are shown in Figure 4.31 and Figure 4.32 respectively.

A reduction of the diffusion tail fit τ values to 70% of the experimental values lowers the QBER which could be obtained with the resonant cavity Si-SPAD to the same value as were achieved with the SSPD. The net bit rate has increased over that which was obtained with the original τ values and as a result is higher than that achieved with the SSPD. A comparison of Figure 4.37 and Figure 4.39 shows that were the PerkinElmer thick junction Si-SPAD with a 200 ps FWHM temporal response to be used in the QKD system it would produce very similar net bit rates as a 70% tail resonant cavity thin junction Si-SPAD with approximately the same QBER at distances of up to 10 km. At distances longer than 10 km the QBER rises rapidly for 200 ps FWHM PerkinElmer thick junction Si-SPAD and the net bit rate suffers a corresponding rapid decrease with transmission distance.

4.2.6 Modelling effect of varying the clock frequency on QKD system parameters

If it can be assumed that the characteristic parameters of the system such as the instrument response and uncertainty in the phase state do not change with the clock frequency then it is possible to model the characteristics of the QKD system for a range of different clock frequencies. Figure 4.40 shows the result of modelling varying the clock frequency for both the SSPD and the resonant cavity thin junction Si-SPAD when using a 2 km long quantum channel.

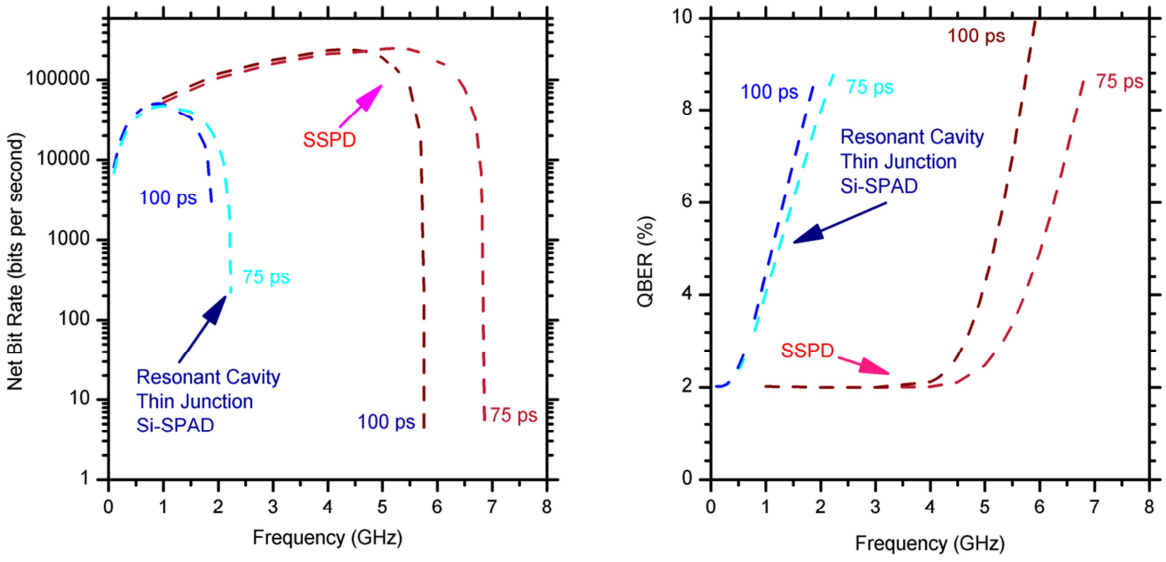

Figure 4.40. A theoretical prediction of the effects of changing the clock frequency of the QKD system on the net bit rate and the quantum bit error rate.

The corresponding decrease in the period of a single bit as the clock frequency increase means that the contribution to the QBER from intersymbol interference increases. The diffusion tail of the resonant cavity Si-SPAD leads to a higher degree of intersymbol interference in comparison to the near Gaussian instrument response of the SSPD resulting in a maximum clock frequency of ~1.5 GHz for the resonant cavity Si-SPAD. The SSPD can be used at frequencies up to ~5.5 GHz in this system when using a 100 ps duration temporal gating window. The approximately Gaussian temporal response of the SSPD means that shorter temporal gate durations can be used and results have been calculated for a 75 ps gate. With the reduced gate the maximum clock frequency for the resonant cavity Si-SPAD increases slightly to ~2 GHz while for the SSPD it increases to ~6.5 GHz. By reducing the size of the temporal gate from 100 ps to 75 ps does not have a significant effect on the baseline QBER although it does push the characteristic QBER verses distance curve to slightly longer distances. However the reduction in the ΔT reduces the $\int_{t-\Delta T/2}^{t+\Delta T/2} P_{Arrival} dt$ term in Equation (4.19) leading to a reduction in the NBR.

4.3 Conclusions

This chapter has looked at a gigahertz clock rate phase encoding QKD system which implements the BB84 protocol. The system is built using optical fibres which allows the system to be integrated into standard optical communication infrastructures.

Custom designed software compensated for changes in the path lengths in the interferometers due to fluctuations in the fibre birefringence caused by environmental effects. This allowed the system to be run autonomously, collecting data for over a 24 hour period. When operated using the SSPD and resonant cavity Si-SPAD detector, net bit rates of 17.75 and 16.7 kbits s^{-1} were obtained respectively and the tuning software managed to maintain the stability for over 19 hours. Similar techniques to compensate for path length drift in Mach-Zehnder interferometers has been demonstrated elsewhere where over a 19 hour period of operation the system was stable for 99% of the time over 20.3 km of installed optical fibre [68].

The novel depolariser technique to remove the effect of environmentally induced birefringent in the quantum channel was also successfully demonstrated in a QKD system for the first time. Photons emitted from the sender had a degree of polarisation of ~10% which enabled the random routing of photons in the receiver when incident on a 50:50 beamsplitter. This enabled Bob to passively and randomly route the photons into one of two Mach-Zehnder interferometers to make a basis set selection. The use of

passive optical components reduced the complexity required in the receiver and eliminated thermal stresses which would destabilise fibre interferometers. The depolariser technique allowed an interferometric visibility of 98% to be achieved even after transmission through standard telecoms fibre and its insensitivity to temperature fluctuations over the course of a day enabled the system to operate continuously during this period.

A variety of single-photon detectors, some commercially available and some research and development, were tested in the system in order to perform a comparison of how detector characteristics can affect a gigahertz clock rate QKD system. It was demonstrated how dark count events, timing jitter, and detection efficiency can influence the lowest QBER and highest net bit rate which can be achieved from the system. The resonant cavity Si-SPAD and the SSPD devices obtained the highest bit rates and transmitted over the longest distances (~18 km) due a combination of low dark count rate (10 Hz for SSPD and 21 Hz for resonant cavity Si-SPAD), high timing performance in the case of the SSPD (Gaussian FWHM ~62 ps) and good detection efficiency of ~18% in the case of the resonant cavity. Although the PerkinElmer device had by far the best detection efficiency, it gave the second lowest net bit rate due to having an inferior FHWM compared to the other devices. This was the most detailed comparison of single-photon detectors in a QKD system to date which experimentally demonstrates the competing effects of timing jitter, dark counts and efficiency have on the QBER and the net bit rate. In the future this could enable detectors to be designed and manufactured with the aim of maximising the performance of a QKD system.

To get a better understanding of the competing effects of timing jitter, dark counts and detecting efficiency a general theoretical model was developed and applied to the different detectors which were used in the QKD system. The model was able to accurately predict the experimental data in Figure 4.31 and Figure 4.32. In particular this model is able to predict the fraction of photon detection events which remain after temporal filtering by treating the arrival time of the photon as a probabilistic event which is characterised by the detector instrumental. This could be beneficial to many photon-counting applications where temporal filtering is carried out, as previously in the literature this fraction was determined empirically. The model was later used to predict the future behaviour of the system in the case of hypothetical realistic detectors and also expected improvements in existing detectors. One of the benefits of the model

is that it can been readily adapted for other QKD systems operating in free-space or optical fibre at 1550 nm by altering Equation (4.16) and by modifying the system instrument response when calculating the probability time of arrival of the photon $P_{arrival}$ which is system and detector dependent.

The theoretical model was also used to investigate the optimal frequency of operation with regard to the maximum bit rate achievable. The maximum clock rate using a temporal window ΔT of 100 ps was ~1.5 GHz and ~5.5 GHz for the resonant cavity thin-junction and SSPD device respectively while using a ΔT of 75 ps a clock rate of ~2 GHz and ~6.5 GHz could be achieved for each detector respectively.

The theoretical model is able to predict that for the 1 GHz clock rate system described here, that if a PerkinElmer thick-junction Si-SPADs with 42% detection efficiency, 198 dark counts per second and pulse read-out electronics modified to give a FWHM timing jitter of 200 ps were to be utilised as the detector, the NBR achieved would exceed that of the 62 ps FWHM timing jitter SSPDs with 10% detection efficiency and ten dark counts per second at distances of up to 15 km. This is only observed because of the 1 GHz clock frequency used in the QKD system. At higher clock rates the temporal intersymbol interference would increase the QBER obtained with the PerkinElmer thick junction Si-SPAD thereby reducing the net bit rate.

The experimental results shown here have only used a single layer meander SSPD[78] Recently, SSPDs embedded in an optical cavity have been reported with an intrinsic efficiency of 57% at a wavelength of 1550 nm and with a practical efficiency greater than 20% [79], [80], [81], [82]. It is possible that further progress will produce SSPDs to match the 850 nm operating wavelength of this system resulting in an increase in the transmission distance and bit rate.

It is also possible to increase the operating clock rate of the QKD system by using a different optical design. Differential phase sifted QKD systems have been shown to operate at clock rates up to 10 GHz, also employing Mach Zehnder interferometers[83]. In this scheme a single photon is transmitted from Alice to Bob in a superposition of three different phase states. The single photons are prepared at Alice and individually transmitted with equal probability into three arms. This system also exhibits the non-interfering peaks visible in the QKD system described here but has been operated at 10

GHz clock frequencies with secure key generation rates of 17 kbit s^{-1} over 105 km of fibre using SSPDs.

Figure 4.41 compares the net bit rate obtained from various QKD systems reported in the literature using various implementations and detectors. The points denoted by ○ and ● represent the results obtained using the thin-junction resonant cavity device and thick junction Si-SPAD previously described in this chapter. The points denoted by ◇ are taken from Hiskett *et al.* which implements a phase encoding system operating at a wavelength of 1550 nm, a clock frequency of 1 MHz and using transition edge sensors with a detection efficiency of 65%[84]. Points denoted by ∆ are taken from *Dixon et al.*[85] and use InGaAs SPADs which operate using self-differencing techniques already described in Chapter 2. The phase encoding system operated at a wavelength of 1550 nm implementing decoys states to overcome the PNS attack. The clock rate of the system was 1 GHz and the detector efficiency was 10% at 1550 nm. Points denoted by ■ and □ are taken from Wang *et al.* [86] and Takesue *et al.* [56] respectively and both use superconducting nanowires implementing the differential phase shift (DPS) QKD protocol described in Chapter 2 and operate at a wavelength of 1550 nm. Wang *et al.* used a Faraday-Michelson interferometer for phase encoding similar to the approach adopted in the "plug-and-play" technique described in Chapter 2. The systems operated with a 2 GHz clock frequency and with a SSPD detection efficiency of 3%. Takesue *et al.* used a standard Mach-Zehnder interferometry arrangement for phase encoding using a 10 GHz clock frequency using SSPDs with a detection efficiency of 0.7%.

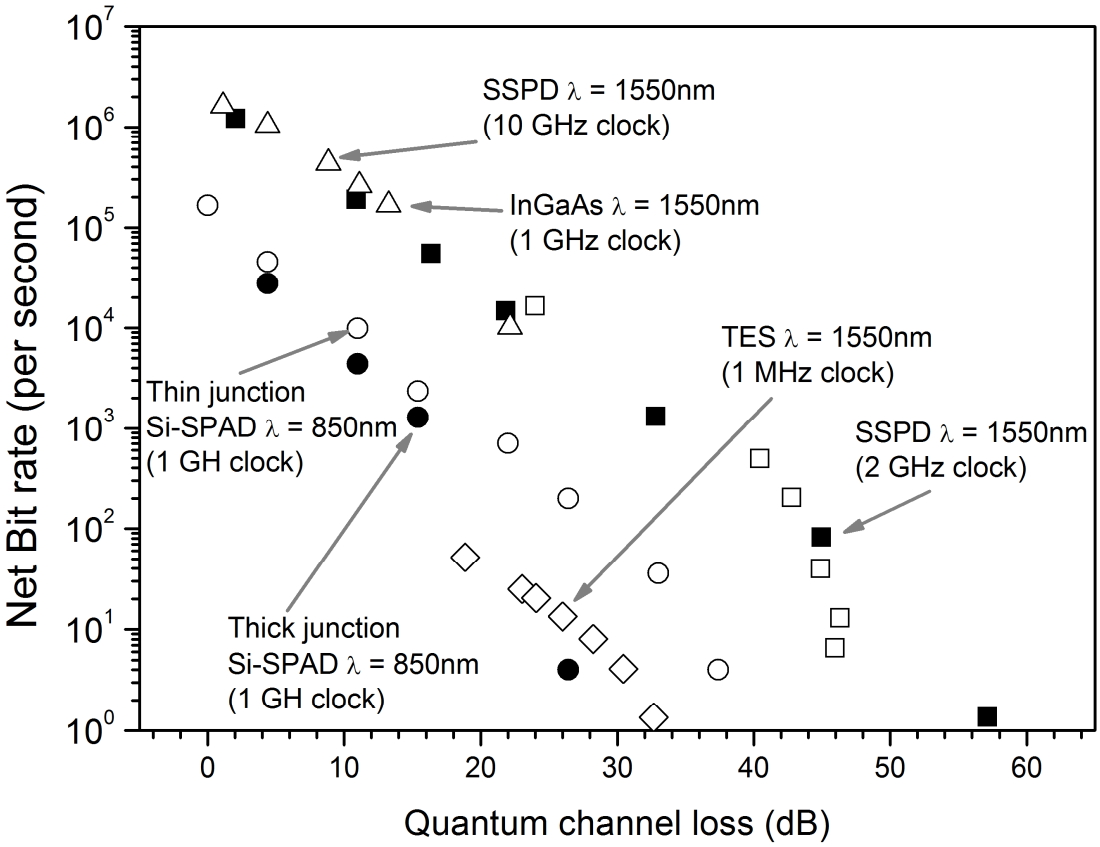

Figure 4.41. The net bit rate obtained from various QKD systems reported in the literature using various implementations and detectors is shown. Points denoted by ○ and ● represent the results obtained using the thin-junction resonant cavity device and thick junction Si-SPAD previously described in this chapter. Points denoted by ◇ are taken from Hiskett et al. [84] which implements a phase encoding system operating at a wavelength of 1550 nm, a clock frequency of 1 MHz and using transition edge sensors with a detection efficiency of 65%. Points denoted by Δ are taken from Dixon et al. [85] and use InGaAs SPADs which operate using self-differencing techniques using. The phase encoding system operated at a wavelength of 1550 nm implementing decoys. The clock rate of the system was 1 GHz and the detector efficiency was 10% at 1550 nm. Points denoted by ■ and □ are taken from Wang et al. [86] and Takesue et al. [56] respectively and both use superconducting nanowires implementing the differential phase shift (DPS) QKD protocol described in Chapter 2 and operate at a wavelength of 1550 nm. Wang et al. used a Faraday-Michelson interferometer for phase encoding, similar to the approach adopted in the "plug-and-play" system. The systems operated with a 2 GHz clock frequency and with a SSPD detection efficiency of 3%. Takesue et al. used a Mach-Zehnder interferometry for phase encoding using a 10 GHz clock frequency using SSPDs with a detection efficiency of 0.7%.

4.4 Acknowledgements

The author would like to thank Dr Robert Collins and Prof Paul Townsend for their help in the design and manufacture of the experimental system presented in this chapter and the theoretical analysis of the system, to Dr Aongus McCarthy for his expertise in free space optics and to María-José García-Martínez for her help in software development and system characterisation. The author would also like to thank Dr Robert Hadfield for supplying the superconducting nanowire detectors and to Dr Michael Tanner, Dr Chandra Natarajan and Catherine Fitzpatrick who provided invaluable technical support with the detectors. The author would like to thank Dr Ivan Rech, Dr Massimo Ghioni and Dr Angelo Gulinatti who provided the experimental resonant cavity thin-junction detector.

References

[1] *"Corning SMF-28 Optical Fiber", Corning,2002, http:// www.corning.com/ WorkArea/showcontent.aspx?id=41261, date accessed:23/5/2012*

[2] I. Choi, R.J. Young, and P.D. Townsend, "*Quantum key distribution on a 10Gb/s WDM-PON"*. Optical Express, 2010. **18**(9): p. 9600-9612.

[3] J.B. Pawley, "*Handbook of biological confocal microscopy"* 1990: Springer.

[4] P. Bishnu, "*Fabrication and modeling of fused biconical tapered fiber couplers"*. Fiber and integrated optics, 2003. **22**(2): p. 97-117.

[5] H.-K. Lo, X. Ma, and K. Chen, "*Decoy state quantum key distribution"*. Physical Review Letters, 2005. **94**(2): p. 230504.

[6] *"High speed VCSEL 2.5 Gbps", Honeywell, New Jersey, U.S.,2001, http://www.datasheetarchive.com/HFE4093-322-datasheet.html, date accessed:24/5/2012*

[7] E.S. Bjorlin, J. Geske, M. Mehta, J. Piprek, and J.E. Bowers, "*Temperature dependence of the relaxation resonance frequency of long-wavelength vertical-cavity lasers"*. Photonics Technology Letters, IEEE, 2005. **17**(5): p. 944-946.

[8] G. Buller, R. Warburton, S. Pellegrini, J. Ng, J. David, L. Tan, A. Krysa, and S. Cova, "*Single-photon avalanche diode detectors for quantum key distribution"*. Optoelectronics, IET, 2007. **1**(6): p. 249-254.

[9] B. Tell, K. Brown‐Goebeler, R. Leibenguth, F. Baez, and Y. Lee, "*Temperature dependence of GaAs‐AlGaAs vertical cavity surface emitting lasers"*. Applied Physics Letters, 1992. **60**(6): p. 683-685.

[10] D.C. Johnson and K.O. Hill, "*Control of wavelength selectivity of power transfer in fused biconical monomode directional couplers"*. Appied Optics, 1986. **25**(21): p. 3800-3803.

[11] M. Fox, "*Quantum optics: an introduction"* 2006: Oxford University Press.

[12] K. Lau, "*Gain switching of semiconductor injection lasers"*. Applied Physics Letters, 1988. **52**(4): p. 257-259.

[13] H. Ito, H. Yokoyama, S. Murata, and H. Inaba, "*Generation of picosecond optical pulses with highly RF modulated AlGaAs DH laser"*. IEEE Journal of Quantum Electronics, 1981. **17**(5): p. 663-670.

[14] J. AuYeung, "*Picosecond optical pulse generation at gigahertz rates by direct modulation of a semiconductor laser"*. Applied Physics Letters, 1981. **38**(5): p. 308-310.

[15] P.V. Mena, J. Morikuni, S.M. Kang, A. Harton, and K. Wyatt, "*A simple rate-equation-based thermal VCSEL model"*. Journal of Lightwave Technology, 1999. **17**(5): p. 865.

[16] W. Nakwaski, "*Thermal aspects of efficient operation of vertical-cavity surface-emitting lasers"*. Optical and quantum electronics, 1996. **28**(4): p. 335-352.

[17] M.B. Gaucher, U. Pfeiffer, and J. Grzyb, "*Advanced millimeter-wave technologies: antennas, packaging and circuits"* 2009: Wiley.

[18] W.H. Steel, "*Interferometry"*. Vol. 1. 1983: Cambridge Univ Pr.

[19] P. Hariharan, "*Basics of interferometry"* 2007: Academic Press.

[20] Y. Zhao, B. Qi, and H.K. Lo, "*Experimental quantum key distribution with active phase randomization"*. Applied Physics Letters, 2007. **90**(4): p. 044106-044106-3.

[21] D.V. Kuksenkov, H. Temkin, and S. Swirhun, "*Polarization instability and relative intensity noise in vertical-cavity surface-emitting lasers"*. Applied Physics Letters, 1995. **67**(15): p. 2141-2143.

[22] D.R. Lutz, "*A passive fiber-optic depolarizer"*. Photonics Technology Letters, IEEE, 1993. **5**(4): p. 463-465.

[23] K. Bohm, K. Petermann, and E. Weidel, "*Performance of Lyot depolarizers with birefringent single-mode fibers"*. Journal of Lightwave Technology, 1983. **1**(1): p. 71-74.

[24] M. Martinelli and J.C. Palais, "*Dual fiber-ring depolarizer"*. Journal of Lightwave Technology, 2001. **19**(6): p. 899.

[25] K. Takada, K. Okamoto, and J. Noda, "*New fiber-optic depolarizer"*. Journal of Lightwave Technology, 1986. **4**(2): p. 213-219.

[26] S. Yamashita and K. Hotate, "*Polarization-independent depolarizers for highly coherent light using Faraday rotator mirrors"*. Journal of Lightwave Technology, 1997. **15**(5): p. 900-905.

[27] J. Sakai, S. Machida, and T. Kimura, "*Degree of polarization in anisotropic single-mode optical fibers: Theory"*. IEEE Transactions on Microwave Theory and Techniques, 1982. **30**(4): p. 334-341.

[28] B. Crosignani and P. Di Porto, "*Degree of polarisation in a birefringent single-mode optical fibre"*. Electronics Letters, 1982. **18**(1): p. 15-16.

[29] I. Malitson, "*Interspecimen comparison of the refractive index of fused silica"*. Journal of the Optical Society of America, 1965. **55**(10): p. 1205-1208.

[30] K. Mochizuki, "*Degree of polarization in jointed fibers: the Lyot depolarizer*". Applied Optics, 1984. **23**(19): p. 3284-3288.

[31] S. Rashleigh and R. Ulrich, "*Polarization mode dispersion in single-mode fibers*". Optics Letters, 1978. **3**(2): p. 60-62.

[32] W.K. Burns and R.P. Moeller, "*Measurement of polarization mode dispersion in high-birefringence fibers*". Optics Letters, 1983. **8**(3): p. 195-197.

[33] I. Kaminow, "*Polarization in optical fibers*". IEEE Journal of Quantum Electronics, 1981. **17**(1): p. 15-22.

[34] C. Marand and P. Townsend, "*Quantum key distribution over distances as long as 30 km*". Optics Letters, 1995. **20**(16): p. 1695.

[35] B.H. Billings, "*A monochromatic depolarizer*". Journal of the Optical Society of America, 1951. **41**(12): p. 966-968.

[36] B. Lyot, Ann. de De L'Observatoire de Paris-Sec. de Meudon, 1929.

[37] W. Burns, "*Degree of polarization in the Lyot depolarizer*". Journal of Lightwave Technology, 1983. **1**(3): p. 475-479.

[38] P. Hariharan, "*Optical Holography: principles, techniques, and applications*" 1996: Cambridge Univ Pr.

[39] *"PC-based time interval analyser GT658", http://www.guidetech.com/gt-658, date accessed:10/5/2012*

[40] L. Mandel and E. Wolf, "*Optical coherence and quantum optics*" 1995: Cambridge Univ Pr.

[41] *"Avtech AVX-CP-2 Power Combiner", Avtech Electrosystems Ltd., USA,http://www.avtechpulse.com/catalog/page102_cat11_avx-sp_rev2.pdf, date accessed:28/5/2012*

[42] S. Bize, Y. Sortais, M. Santos, C. Mandache, A. Clairon, and C. Salomon, "*High-accuracy measurement of the 87Rb ground-state hyperfine splitting in an atomic fountain*". EPL (Europhysics Letters), 1999. **45**: p. 558.

[43] J.C. Bienfang, A.J. Gross, A. Mink, B. Hershman, A. Nakassis, X. Tang, R. Lu, D. Su, C.W. Clark, and C.J. Williams, "*Quantum key distribution with 1.25 Gbps clock synchronization*". Arxiv preprint quant-ph/0405097, 2004.

[44] K.J. Gordon, V. Fernandez, P.D. Townsend, and G.S. Buller, "*A short wavelength gigahertz clocked fiber-optic quantum key distribution system*". IEEE Journal of Quantum Electronics, 2004. **40**(7): p. 900-908.

[45] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, and J.G. Rarity, "*Experimental*

demonstration of free-space decoy-state quantum key distribution over 144 km". Physical Review Letters, 2007. **98**(1): p. 10504.

[46] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "*Free-space quantum key distribution with entangled photons"*. Applied Physics Letters, 2006. **89**: p. 101122.

[47] T. Scheidl, R. Ursin, A. Fedrizzi, S. Ramelow, X.S. Ma, T. Herbst, R. Prevedel, L. Ratschbacher, J. Kofler, and T. Jennewein, "*Feasibility of 300 km quantum key distribution with entangled states"*. New Journal of Physics, 2009. **11**: p. 085002.

[48] N. Takeuchi, N. Sugimoto, H. Baba, and K. Sakurai, "*Random modulation cw lidar"*. Applied Optics, 1983. **22**(9): p. 1382-1386.

[49] C. Nagasawa, M. Abo, H. Yamamoto, and O. Uchino, "*Random modulation cw lidar using new random sequence"*. Applied Optics, 1990. **29**(10): p. 1466-1470.

[50] P.A. Hiskett, C.S. Parry, A. McCarthy, and G.S. Buller, "*A photon-counting time-of-flight ranging technique developed for the avoidance of range ambiguity at gigahertz clock rates"*. Optics Express, 2008. **16**(18): p. 13685-13698.

[51] J. Bienfang, A. Gross, A. Mink, B. Hershman, A. Nakassis, X. Tang, R. Lu, D. Su, C. Clark, and C. Williams, "*Quantum key distribution with 1.25 Gbps clock synchronization"*. Optics Express, 2004. **12**(9): p. 2011-2016.

[52] K.J. Gordon, V. Fernandez, G.S. Buller, I. Rech, S.D. Cova, and P.D. Townsend, "*Quantum key distribution system clocked at 2 GHz"*. Optics Express, 2005. **13**(8): p. 3015-3020.

[53] H. Dautet, P. Deschamps, B. Dion, A.D. MacGregor, D. MacSween, R.J. McIntyre, C. Trottier, and P.P. Webb, "*Photon counting techniques with silicon avalanche photodiodes"*. Applied Optics, 1993. **32**(21/20).

[54] M. Ghioni, G. Armellini, P. Maccagnani, I. Rech, M.K. Emsley, and M.S. Ünlü, "*Resonant-cavity-enhanced single photon avalanche diodes on double silicon-on-insulator substrates"*. Journal of Modern Optics, 2009. **56**(2-3): p. 309-316.

[55] R. Collins, R. Hadfield, V. Fernandez, S. Nam, and G. Buller, "*Low timing jitter detector for gigahertz quantum key distribution"*. Electronics Letters, 2007. **43**(3): p. 180-181.

[56] H. Takesue, S. Nam, Q. Zhang, R. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "*Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors"*. Nature Photonics, 2007. **1**(6): p. 343-348.

[57] A. Tanaka, S. Takahashi, W. Maeda, A. Tajima, M. Fujiwara, M. Sasaki, S. Nam, B. Baek, Y. Nambu, and K.I. Yoshino, "*Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength-division multiplexing clock synchronization"*. Optics Express, 2008. **16**(15): p. 11354-11360.

[58] *"SPCM-AQR single photon counting module Perkin Elmer datasheet", 2005, http://www.htds.fr/doc/optronique/militaireAerospace/SPCM-AQR.pdf, date accessed:02/10/2012*

[59] *"MPD PDM series Micro Photon Devices Datasheet", http:// www .microphotondevices.com/media/pdf/PDM v3 3.pdf, date accessed:02/10/2012*

[60] *"IDQ id100 series IDQ Datasheet", http://www.perkinelmer.com/ph/ Category/Category/cat1/IDSMI_TAXONOMY_DELETIONS/cat2/IND_SE_CAT _Single%20photon%20Counting%20Modules%20SPCM_001/key/10613, date accessed:02/10/2012*

[61] S. Miki, M. Fujiwara, M. Sasaki, B. Baek, A.J. Miller, R.H. Hadfield, S.W. Nam, and Z. Wang, "*Large sensitive-area NbN nanowire superconducting single-photon detectors fabricated on single-crystal MgO substrates"*. Applied Physics Letters, 2008. **92**: p. 061116.

[62] R. Radenbaugh, "*Refrigeration for superconductors"*. Proceedings of the IEEE, 2004. **92**(10): p. 1719-1734.

[63] S. Pellegrini, G.S. Buller, J.M. Smith, A.M. Wallace, and S. Cova, "*Laser-based distance measurement using picosecond resolution time-correlated single-photon counting"*. Measurement Science and Technology, 2000. **11**: p. 712.

[64] W. Andrew M, Y. Jing, K. Nils J, M.C. Aongus, C. Robert J, and B. Gerald S, "*Full Waveform Analysis for Long-Range 3D Imaging Laser Radar"*. EURASIP Journal on Advances in Signal Processing, 2010. **2010**.

[65] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "*Quantum cryptography"*. Reviews of Modern Physics, 2002. **74**(1): p. 145-195.

[66] C. Gobby, Z. Yuan, and A. Shields, "*Quantum key distribution over 122 km of standard telecom fiber"*. Applied Physics Letters, 2004. **84**: p. 3762.

[67] K. Kojima, K. Kyuma, and T. Nakayama, "*Analysis of the spectral linewidth of distributed feedback laser diodes"*. Journal of Lightwave Technology, 1985. **3**(5): p. 1048-1055.

[68] Z. Yuan and A. Shields, "*Continuous operation of a one-way quantum key distribution system over installed telecom fibre"*. Optics Express, 2005. **13**(2): p. 660-665.

[69] G. Brassard and L. Salvail. "*Secret-key reconciliation by public discussion"*. in *Advances in cryptography- Eurocrypt '93, Lecture Notes in Computer Science*. 1994. Springer.

[70] P. Gronberg and P. Jonsson. "*Key reconciliation in quantum key distribution"*. in *Sensor Technology Technical Report FOIR-1743-SE* 2005. Totalförsvarets Forskningsinstitut.

[71] C. Shannon, "*A mathematical theory of communication"*. Bell Labs System Technical Journal 1948. **27**(1): p. 379-423, 623-656.

[72] P. Webb and R. McIntyre, "*Single photon detection with avalanche photodiodes"*. Bulletin of the American Physical Society, Ser. II, 1970. **15**: p. 813.

[73] S. Cova, M. Ghioni, A. Lotito, I. Rech, and F. Zappa, "*Evolution and prospects for single-photon avalanche diodes and quenching circuits"*. Journal of Modern Optics, 2004. **51**(9): p. 1267-1288.

[74] I. Rech, I. LaBanca, M. Ghioni, and S. Cova, "*Modified single photon counting modules for optimal timing performance"*. Review of Scientific Instruments, 2006. **77**: p. 033104.

[75] A. Restelli, J.C. Bienfang, C.W. Clark, I. Rech, I. Labanca, M. Ghioni, and S. Cova, "*Improved Timing Resolution Single-Photon Detectors in Daytime Free-Space Quantum Key Distribution With 1.25 GHz Transmission Rate"*. IEEE Journal of Selected Topics in Quantum Electronics, 2010. **16**(5): p. 1084-1090.

[76] A. Restelli, J.C. Bienfang, C.W. Clark, I. Rech, I. Labanca, M. Ghioni, and S. Cova, "*Improved timing resolution single-photon detectors in daytime free-space quantum key distribution with 1.25 GHz transmission rate"*. Selected Topics in Quantum Electronics, IEEE Journal of, 2010. **16**(5): p. 1084-1090.

[77] G.S. Buller and R.J. Collins, "*Single-photon generation and detection"*. Measurement Science and Technology, 2010. **21**: p. 012002.

[78] P.J. Clarke, R.J. Collins, P.A. Hiskett, P.D. Townsend, and G.S. Buller, "*Robust gigahertz fiber quantum key distribution"*. Applied Physics Letters, 2011. **98**(13): p. 131103-131103-3.

[79] X. Hu, T. Zhong, J.E. White, E.A. Dauler, F. Najafi, C.H. Herder, F.N.C. Wong, and K.K. Berggren, "*Fiber-coupled nanowire photon counter at 1550 nm with 24% system detection efficiency"*. Optics Letters, 2009. **34**(23): p. 3607-3609.

[80] M. Tanner, C. Natarajan, V. Pottapenjara, J. O'Connor, R. Warburton, R. Hadfield, B. Baek, S. Nam, S. Dorenbos, and E.B. Ureña, "*Enhanced telecom wavelength single-photon detection with NbTiN superconducting nanowires on oxidized silicon"*. Applied Physics Letters, 2010. **96**: p. 221109.

[81] S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, and Z. Wang, "*Multichannel SNSPD system with high detection efficiency at telecommunication wavelength"*. Optics Letters, 2010. **35**(13): p. 2133.

[82] S. Miki, M. Takeda, M. Fujiwara, M. Sasaki, and Z. Wang, "*Compactly packaged superconducting nanowire single-photon detector with an optical cavity for multichannel system"*. Optics Express, 2009. **17**(26): p. 23557-23564.

[83] H. Takesue, E. Diamanti, C. Langrock, M. Fejer, and Y. Yamamoto, "*10-GHz clock differential phase shift quantum key distribution experiment"*. Optics Express, 2006. **14**(20): p. 9522-9530.

[84] P. Hiskett, D. Rosenberg, C. Peterson, R. Hughes, S. Nam, A. Lita, A. Miller, and J. Nordholt, "*Long-distance quantum key distribution in optical fibre"*. New Journal of Physics, 2006. **8**: p. 193.

[85] A.R. Dixon, Z.L. Yuan, J.F. Dynes, A.W. Sharpe, and A.J. Shields, "*Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate"*. Optics Express, 2008. **16**(23): p. 18790-18979.

[86] S. Wang, W. Chen, J.F. Guo, Z.Q. Yin, H.W. Li, Z. Zhou, G.C. Guo, and Z.F. Han, "*2-GHz clock quantum key distribution over 260 km of standard telecom fiber"*. Optics Express, 2012. **37**(6): p. 1008-1010.

Chapter 5

Quantum Digital Signatures

5.1 Introduction to classical digital signatures

Digital signatures can be thought of as an analogue of a handwritten signature but guarantees a much higher level of security over their handwritten counterpart. Digital signatures are widely used in today's world and are used for signing legal contracts, authenticating legal software for download and they also allow the transmission of public keys and as a result are used in the previously discussed public key cryptography discussed in Chapter 2. A digital signature scheme is usually composed of a signer and one, or potentially more verifiers. The scheme is commenced by the signer running a key generation algorithm to produce a pair of keys (p_{key}, s_{key}) where p_{key} is the signer's public key and s_{key} is the signer's private key. The signer then publically announces the public key and one assumes the verifier is in procession of an authentic copy of the public key. The digital scheme then allows the signer to certify a message such that any other party who is in procession of p_{key}, can then verify that the message originated from the signer and has not been tampered with. Figure 5.1 shows an outline of how the scheme works in principle.

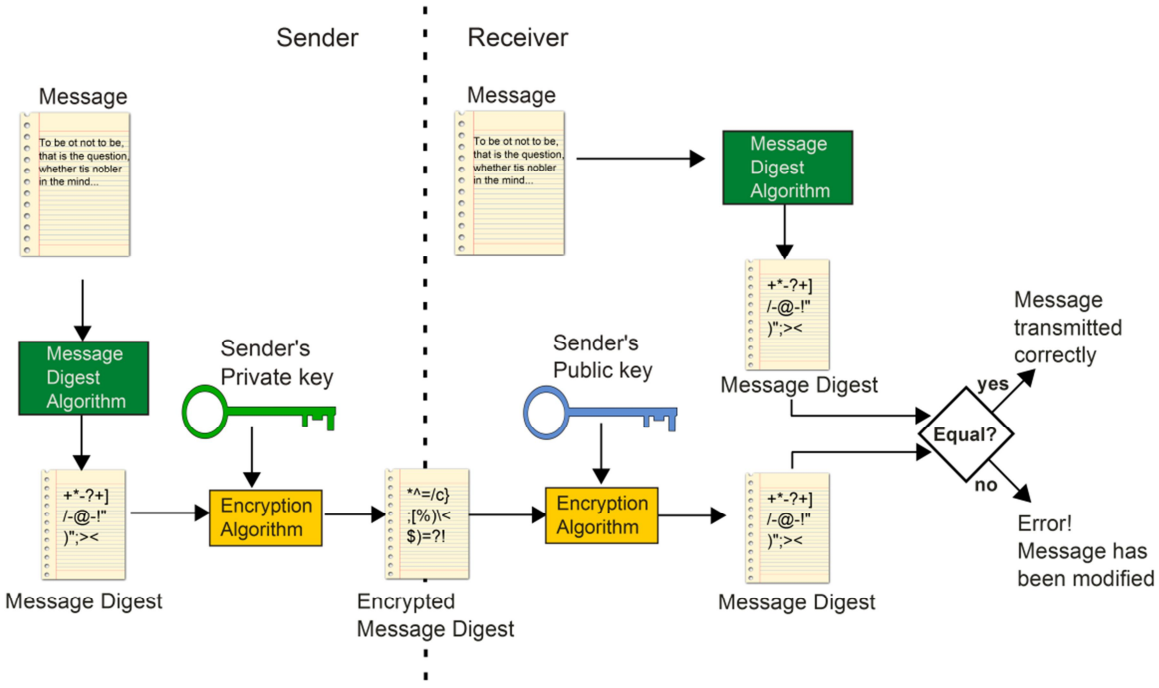

Figure 5.1. Outline of a digital signatures scheme [1].

Digital signatures fall under the branch of public key cryptography where a party, a signer in the case of digital signatures, only has to distribute a key over a public but authenticated channel. Two important aspects of digital signatures are that they are publically verifiable and have the property of non-repudiation. Publically verifiable means that if a receiver verifies that a message is authentic then other parties who receive the signed message also agree on it being legitimate. Non-repudiation means that once a signer signs a message they cannot later deny that the message was sent from them. This feature is often used when a recipient then needs to prove to a third party, a judge, that the signer did certify a message, assuming that the judge is also in procession of the public key [2].

5.2 Security of digital signatures

The security of digital signatures is based on the unproven assumptions in the theory of computational complexity, namely the idea that $P \neq NP$. P represents decision problems that can be efficiently solved while NP represent decision problems in which the solutions have proofs which can be efficiently checked [3]. A digital signatures scheme is not secure against an adversary with unlimited computational power or unlimited time. It is quite common to use a security parameter k which can be used to quantify the level of security of the scheme. The signer passes this parameter as the input to the key-generation algorithm and the length of the public and private key will depend on k. To satisfy a level of computational security a digital signature scheme has the property that a probabilistic polynomial-time (PPT) adversary will only succeed in forging a signature with negligible probability.

5.3 Digital signature architect

The digital scheme should consist of three polynomial-time algorithms ($Gen, Sign, Vrfy$). The key generation algorithm Gen takes the security parameter k as its input and outputs the public key p_{key} or verification key, and the private key/signing key/secret key s_{key}. For a given security parameter k the signing algorithm $Sign$ uses the private key s_{key} and the message m as its input and outputs a signature σ, $\sigma \leftarrow Sign_{s_{key}}(m)$. Finally the verification algorithm $Vrfy$ takes the public key p_{key}, the message m and the signature signal and outputs a single bit b, $b = Vrfy_{p_{key}}(m, \sigma)$, with b=1 meaning to accept and b=0 to reject the signature. The signer runs the Gen algorithm to obtain the keys p_{key} and s_{key}. When a sender wants to send a message m it runs $Sign_{s_{key}}(m) \rightarrow \sigma$ and sends (σ, m) to the receiver. The receiver who already knows the public key p_{key}

is able to verify the authenticity of the message by checking the value $Vrfy_{p_{key}}(m,\sigma)$. This allows it to be proved that the sender sent m and that it was not modified in transit [2]. Some of the one-way functions which digital signatures relies on are discussed in the next section.

5.4 Cryptographic one-way functions

A regular occurrence in cryptography and digital signature schemes are one-way functions. These are functions which are easy to compute in one direction but harder to reverse without some *a priori* knowledge. A computational problem is considered *easy* if it can be solved in polynomial time.

5.4.1 Trapdoor functions

Diffie and Hellman introduced the idea of trapdoor one-way functions for use in asymmetric encryption and public key distribution [4]. They described a trapdoor function with the following properties;

1. given a description of the function $f(x)$ and x it is computationally feasible to compute $y = f(x)$
2. given $f(x)$ and $y = f(x)$ it is computationally infeasible to compute $f^{-1}(y)$
3. given $f(x)$, $y = f(x)$ and a parameter z it is computationally feasible to compute $x = f^{-1}(y)$.

The calculation of $y = f(x)$ is the process of enciphering the plaintext with the public key and the calculation of $x = f^{-1}(y)$ is the deciphering of the ciphertext with the private key. Without the knowledge of trapdoor information z it is computational infeasible to invert the function [5].

5.4.2 Prime factorisation and discrete logarithm problem

The security of classical cryptography such as RSA relies upon the difficulty of integer factorisation problems. The integer factorisation problems states that given a positive integer n find its primes factors such that n can be written as $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ where p_i are distinct primes and $e_i \geq 1$. The most straight forward factorising algorithm is by trial division. This can be attempted by trail division by all "small" primes where "small" depends on the size of n. In a worst case scenario trail division can be attempted by all primes up to $\sqrt{n}$. In this case trail division will completely factor n but the procedure will take above $\sqrt{n}$ divisions when n is a product of two primes which are the same size. To factor n completely takes $O(p + \log n)$ divisions where p

is the second largest prime factor of n. This method is completely infeasible for large enough integers [6]. The most efficient classical algorithm of factorising integers over 100 digits is the General Number Field Sieve (GNFS) and was used to factor a 130 bit digit number in the RSA factorising challenge [7].

The discrete logarithm problem involves the branch of mathematics called group theory. Let g^n denote the element in the infinite group G where g is multiplied by itself n times. The discrete logarithm problem states that if $g \in G$ and another element $h \in G$, find an integer x such that $g^x = h$. Like the factoring problem, the discrete logarithm problem is believed difficult to compute and is used in the Diffie-Hellman key exchange.

5.4.3 Cryptographic hash functions

Cryptographic hash functions are used extensively in the construction of secure digital signature schemes. They essentially compress a message to produce a condensed version called a message digest. This is particularly useful when seeking to improve a signature scheme that can sign k-bit messages into one that can sign message of arbitrary length. In order to sign a long message all that is required is to hash all messages before signing them. These functions have the following properties, they should be preimage resistant which means that given a hash h it is computationally infeasible to find a message m such that $h = hash(m)$, second-preimage resistant meaning that given a input m_1 it is computationally infeasible to find another input m_2 with $m_1 \neq m_2$ such that $hash(m_1) = hash(m_2)$ and finally collision resistant meaning that it should be computationally infeasible to find two messages m_1 and m_2 such that $hash(m_1) = hash(m_2)$. The birthday "paradox" places an upper bound on the collision resistance. The number of messages that is needed to hash to find a collision is approximately equal to the square root of the number of possible output values, i.e. $2^{n/2}$ where n is the number of output bits of the hash function The secure hash algorithm (SHA-1) is the most widely used hash algorithm in use today and produces a 160 bit message digest and has a collision resistant of about 2^{80} [8].

5.5 History of digital signatures and digital schemes

The concept of digital signatures was first born out of work that Ronald Rivest, Adi Shamir and Len Adleman outlined in their 1978 paper [9]. If Bob wants to send a signed message M to Alice he first creates his signature S for the message M by

using his decryption function D_B, $S = D_B(M)$. He then encrypts S using E_A, Alice's encryption process and sends the result $E_A(S)$ to Alice. Alice then decrypts with D_A to obtain S. The message is obtained by the encryption procedure of the sender E_B, $M = E_B(S)$. Bob cannot refute having sent the message since only he could create $S = D_B(M)$. Alice can also convince a third party acting as a judge that $M = E_B(S)$ which is proof that Bob signed the message. Given a message M the ciphertext C is the remainder when M^e is divided by n such that $C \equiv E(M) = M^e \bmod(n)$, where n is the product of two primes p and q and e is a positive integer. The value of n is made public but p and q are kept private. Together e and n are the encryption key. Decryption can be performed by $D(C) \equiv C^d \bmod(n)$ where d and n are the decryption keys. The value d is chosen such that the greatest common divisor (gcd) of d and $(p-1)\cdot(q-1) = 1$.

5.5.1 Lamport one-time signature

Lamport's one-time digital scheme was first purposed in 1979 [10]. The scheme is based on cryptographic hash functions (f) which are mathematically infeasible to invert. For the secret key, each bit that a signer S may wish to sign in the future they choose two numbers $sk_{(0)}^{(i)}$ and $sk_{(1)}^{(i)}$, chosen randomly from the domain of f. The signer then announces $pk^{(i)} = f\left(sk_b^{(i)}\right)$ as her public key. Later to sign that the value of the i-th bit is b she announces the value $sk_b^{(i)}$. The receiver can authenticate for each bit b and the supposed signature s_i by checking if $f(s_i) \stackrel{?}{=} pk_{b_i}^{(i)}$. Figure 5.2 shows an example of signing a 3 bit message. The public key consists of 6 elements $y_{1,0}, y_{1,1}, y_{2,0}, y_{2,1}, y_{3,0}, y_{3,1}$ which are computed from the function f using the private keys $x_{1,0}, x_{1,1}, x_{2,0}, x_{2,1}, x_{3,0}, x_{3,1}$. In matrix notation this is given by Equation (5.1).

$$pk = \begin{pmatrix} y_{1,0} & y_{2,0} & y_{3,0} \\ y_{1,1} & y_{2,1} & y_{3,1} \end{pmatrix} \qquad sk = \begin{pmatrix} x_{1,0} & x_{2,0} & x_{3,0} \\ x_{1,1} & x_{2,1} & x_{3,1} \end{pmatrix} \qquad \text{Equation (5.1)}$$

To sign a message $m = m_1 \| m_2 \| m_3$ where m_i is a single bit and $\|$ represents string concatenation, the signer publishes x_{i,m_i} for $1 \le i \le 3$. The signature s_i consists of $x_{1,m_i}, x_{2,m_i}, x_{3,m_i}$. The verifier accepts the signature only if $f(x_i) \stackrel{?}{=} y_{i,m_i}$. The scheme is called a one-time signature as each part of the secret key can only be used once. The very large length of the public keys make the scheme impractical as the public keys have to be transmitted reliably at the beginning [2].

Signing $m = 011$**:**

$$sk = \begin{pmatrix} \boxed{x_{1,0}} & x_{2,0} & x_{3,0} \\ x_{1,1} & \boxed{x_{2,1}} & \boxed{x_{3,1}} \end{pmatrix} \Rightarrow \sigma = (x_{1,0}, x_{2,1}, x_{3,1})$$

Verifying for $m = 011$ **and** $\sigma = (x_1, x_2, x_3)$**:**

$$pk = \left.\begin{pmatrix} \boxed{y_{1,0}} & y_{2,0} & y_{3,0} \\ y_{1,1} & \boxed{y_{2,1}} & \boxed{y_{3,1}} \end{pmatrix}\right\} \Rightarrow \begin{array}{l} f(x_1) \stackrel{?}{=} y_{1,0} \\ f(x_2) \stackrel{?}{=} y_{2,1} \\ f(x_3) \stackrel{?}{=} y_{3,1} \end{array}$$

Figure 5.2. Lamport digital signature scheme for signing a three bit message m=011 [2].

5.6 Security concerns with classical digital signatures

As seen previously digital signatures have been shown to be able to sign a message so that a receiver can authenticate the sender and also verify that the contents were not altered. The security of such a scheme is based on the computational difficulty of reversing certain one-way functions but such security is not guaranteed into the future with possible better algorithms or quantum computers [11], [12]. The paradox of these functions is that it is not possible to prove that they are non-invertible as the proof would suggest that they are not one-way to begin with [13]. The MD5 message digest algorithm, proposed by Rivest in 1994, is a cryptographic hash function that produces a 128 bit message digest [8]. For over a decade this function was considered to be resistant to collisions. A collision is a pair of distinct data values x and x' for which $H(x) = H(x')$. However in 2005 Chinese cryptographers discovered a new technique for discovering collisions in this algorithm which can be done in 5 minutes to an hour using an IBM P690 multiprocessor server [14]. In 2012 Microsoft announced that the authors of the Fame malware used collisions in MD5 to forge a Windows code signing certificate [15]. As a result the National Institute of Standards and Technology (NIST) recommends that such a function is no longer suitable for Secure Socket Layer (SLL) certificates or digital signatures [16].

5.7 Security and information theory background for quantum digital signatures

5.7.1 Entropy and information

As briefly discussed in Chapter 2 the Shannon entropy and information are closely related and are used extensively in cryptography for assessing the security of a system.

The link between entropy in thermodynamics and information was firmly established by Landauer's principle which states that the erasure of an unknown bit requires at least $kT\ln 2$ of heat per lost bit [17]. The cross over between the field of mathematics and physic is very apparent in cryptography as information is often described by the branch of probability. If the value of a random variable X is measured then the Shannon entropy of X quantifies how much information on average we gain by measuring X. In relation to statistical mechanics and information theory, entropy can be thought of as a measure of missing information, the information that could be gained if a complete measure of a system could be performed [18], [19]. The entropy of a system is often written as a probability distribution $p_1,\ldots p_n$ The Shannon entropy of such a probability distribution is given by the following [20]

$$H(X) \equiv H(p_1 \ldots p_n) \equiv -\sum_{i=1}^{n} p(x_i)\log p(x_i) \qquad \text{Equation (5.2)}$$

where $p(x_i)$ is the probability of the outcome of x_i. In simple terms, if an information source produces a string of $X_1, X_2 \ldots X_n$ values which are independent random variables then the Shannon entropy can be thought of as the minimal physical resources that is required to store all the information and which can later be fully reproduced. The entropy associated with a two-outcome random variable is given by

$$H_{binary}(X) = -p\log p - (1-p)\log(1-p) \qquad \text{Equation (5.3)}$$

p and $p-1$ are the probability of the two outcomes. One of the outcomes of the Shannon entropy is that if an event occurs with probability $p-1$ or with probability $p=0$ no information is gained by making a measurement. The function reaches a maximum at $p=0.5$, where with a unbiased coin toss with a heads or a tails outcome maximum information is gained by performing a measurement. This means that one bit of information is needed to communicate the outcome of the coin toss. However in the case of a fair die at least $\log_2(6)$ bits is required. More information is obtained when rolling a die than is obtained with a coin toss. The probability of obtained heads with a coin is $1/2$ while the probability of rolling a 3 with a die is $^1/_6$ [21].

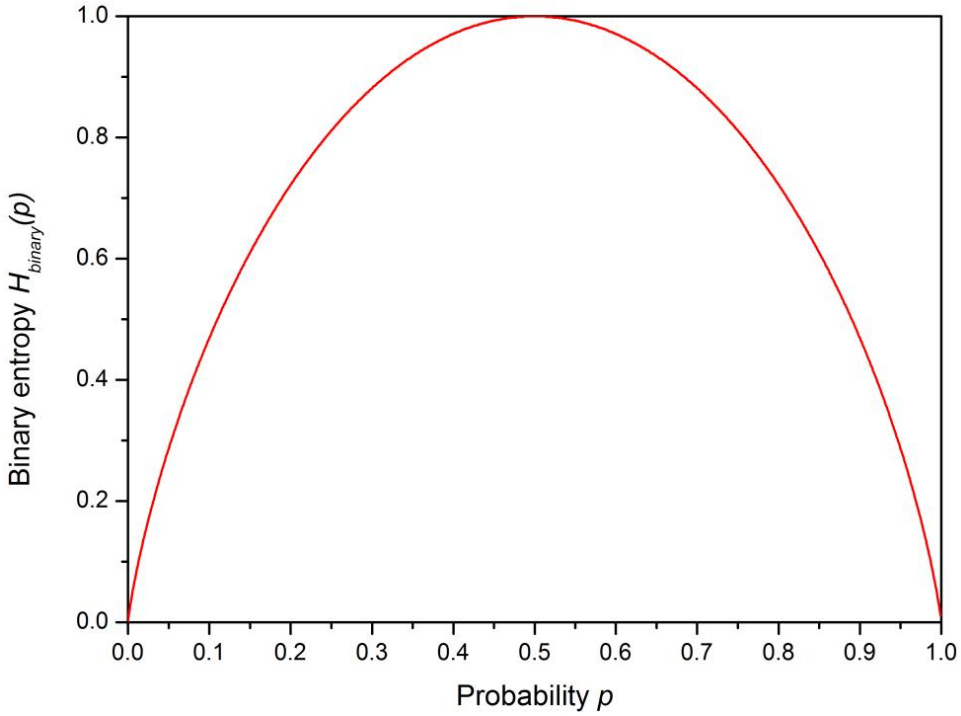

Figure 5.3. The binary entropy function. The function reaches a maximum value at probability p=0.5.

Two other important concepts relating to entropy which are used to calculate security bounds for quantum information systems are conditional entropy and mutual information [22], [23]. It is usual to being by defining X and Y as two random variables. The entropy of X on the condition that we know Y is given by

$$H(X|Y) = H(X,Y) - H(Y) \qquad \text{Equation (5.4)}$$

where $H(X,Y)$ is the joint entropy. This is a measure of the average uncertainty of X given that we know the value of Y. The mutual information quantifies how much information X and Y have in common and is given by

$$H(X:Y) \equiv H(X) + H(Y) - H(X,Y) \qquad \text{Equation (5.5)}$$

5.7.2 Von Neumann entropy

In classical information theory the Shannon entropy is used to measure the uncertainty of an random variable whereas the von Neumann entropy is the quantum mechanics equivalent. It is given by

$$S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho) \qquad \text{Equation (5.6)}$$

where ρ is the quantum state and *tr* represents the trace of the matrix. If the eigenvalues of ρ are given by λ_x then the von Neumann's entropy may be recast as

$$S(\rho) = -\sum_x \lambda_x \log \lambda_x \qquad \text{Equation (5.7)}$$

The Shannon noiseless coding theorem states that given n random variables with entropy $H(x)$, they can be compressed into $nH(x)$ bits with minimum risk of information loss as $n \to \infty$. If however they are compressed into fewer than $nH(x)$ bits then it is likely that information will be lost. Likewise n qubit messages from a quantum source with a von Neumann entropy $S(\rho)$ can be compressed into a maximum of $nS(\rho)$ [24]. If the state ρ is a pure state ρ_{state} then the von Neumann entropy $S(\rho_{state}) = 0$, which means that further repeated measurements of the state yields no further information [18].

5.8 Quantum gates in quantum computation

Quantum computers offer the possibility of a remarkable increase in the speed of computers for performing calculations. Quantum algorithms can make use the fact that quantum bits, or qubits, can be a superposition of a 1 or 0. One of these quantum algorithms is based on Shor's quantum Fourier transform which enables an exponential increase in speed over classical algorithms for factorisation [25]. The other is based on Grover's algorithm for quantum searching [12], [26]. In order to perform such calculations there is a need for the quantum equivalent of logic gates in classical computation. Two such quantum gates are discussed in sections 5.8.1 and 5.8.2 which are needed to describe the comparison of two quantum states via the "swap test".

5.8.1 Fredkin gate

The Fredkin gate, shown schematically in Figure 5.4, is a type of logic gate used in quantum mechanics. It has three inputs a, b, c and has three outputs a', b', and c'. The bit value c is called the control bit and has the property of not being altered by the gate such that $c = c'$. The control bit determines which action is to be performed on a and b. If $c = 0$ then a and b are not altered by the gate such that $a = a'$ and $b = b'$. If on the other hand c =1 then the bits a and b are swapped at the output such that $a' = b$ and $b' = a$. The Frekin gate has the property of being reversible and being able to be used as a universal logic gate.

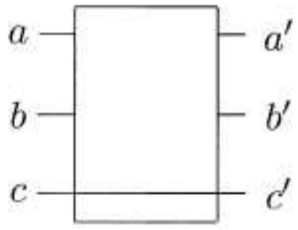

Figure 5.4. Fredkin gate. The output bits a and b depend on the control bit c which is unaltered by the gate. If $c = 0$ then the inputs a and b are not altered but if the control bit is set to 1 then the input bits are swapped such that $a' = b$ and $b' = a$

.

5.8.2 Hadamard gate

The Hadamard gate is given by the following matrix,

$$H_{gate} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \text{Equation (5.8)}$$

and it transforms $|0\rangle$ into $1/\sqrt{2}\left(|0\rangle + |1\rangle\right)$ and $|1\rangle$ into $1/\sqrt{2}\left(|0\rangle - |1\rangle\right)$ [27], [28]. The transform itself can be thought of as a generalised class of Fourier transform and can be thought simply as a 90° rotation about the x and z axis on the Bloch sphere. It can be implemented using linear optics such as Mach-Zehnder interferometer. The Hadamard gate has the useful property that if H_{gate} is independently applied to n qubits which are all initial prepared in the same state $|0\rangle$ then the state produced is a superposition of all the integers from 0 to $2^n - 1$. Therefore a superposition which contains exponentially many terms can be prepared using only a polynomial number of operations [24].

5.9 Determining quantum states and the Holevo bound

The property of the inability of quantum states to be copied and their inability to be distinguished unambiguously can be quantified by the Holevo bound. The laws of quantum mechanics make it impossible to perfectly distinguish between two non-orthogonal quantum states. This can be thought of in relation to the accessible information. If a sender Alice prepares a quantum state $|\phi\rangle$ with probability p and prepares the state $|\varphi\rangle$ with probability $1-p$ then the accessible information to the receiver Bob must be less than $H(p)$ as there is no way to distinguish the state with absolute certainty. In the classical scenario if Alice prepares a bit 0 with probability p and a bit 1 with probability $1-p$ then there is no physical reason why Bob cannot determine the two states and his mutual information is given by $H(p)$, which is the entropy in which the state was prepared. Formally stated the Holevo bound is given by

$$H(X:Y) \leq S(\rho) - \sum_x p_x S(\rho_x) \qquad \text{Equation (5.9)}$$

This describes the scenario where Alice prepares a quantum state $|\rho_x\rangle$ where $x = 1,\ldots,n$ each given by probabilities $p_1,\ldots,p_n$ and Bob performs a measurement on the state where the outcome is Y. $\rho = \sum_x p_x \rho_x$. His accessible information is bounded by the term on the right of Equation (5.9) and is often called the Holevo quantity χ. If the sates ρ_x are not orthogonal then the Holevo bound implies that the mutual information $H(X:Y)$ is always less that $H(X)$ which means that it is impossible for Bob to determine X with 100% certainty based on his measurement of X. This can be demonstrated when Alice prepares two states $|0\rangle$ and $\cos\theta|0\rangle + \sin\theta|1\rangle$ depending on the outcome of a coin toss. The combined state in the $|1\rangle$ $|0\rangle$ basis is given by

$$\rho = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} \cos^2\theta & \cos\theta\sin\theta \\ \cos\theta\sin\theta & \sin^2\theta \end{pmatrix} \qquad \text{Equation (5.10)}$$

The Holevo bound is plotted as a function of the angle θ in Figure 5.5 and reaches a maximum at $\theta = \pi/2$ which corresponds to the two states being orthogonal to each other. It is only in this scenario that Bob is able to distinguish the states with 100% certainty [13].

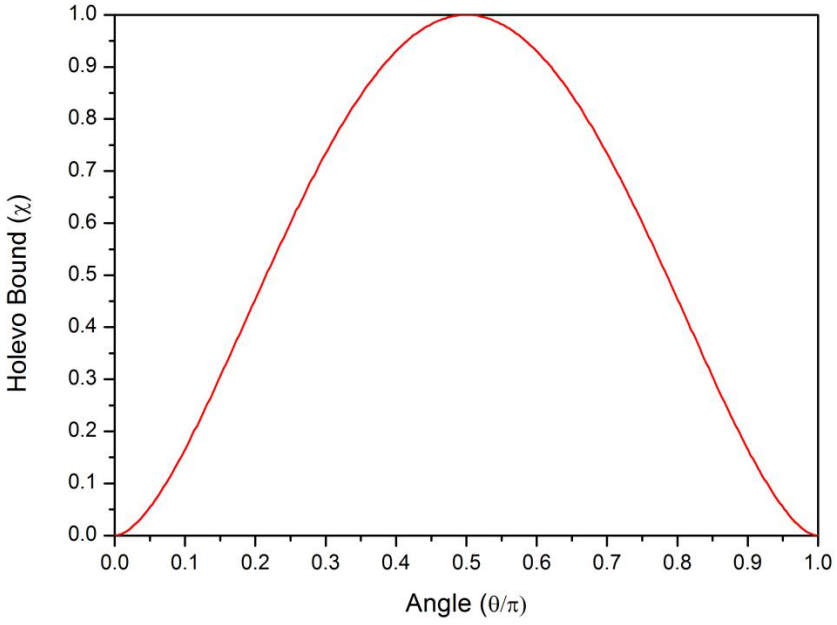

Figure 5.5. Holevo bound as a function of angle when the states $|0\rangle$ and $\cos\theta|0\rangle + \sin\theta|1\rangle$ are prepared with equal probability. A maximum is reached when $\theta = \pi/2$ which occurs when the states are orthogonal to each other and Bob is able to distinguish the states with 100% certainty.

5.10 The current state of quantum digital signatures

In 2001 Gottesman and Chaung established a scheme for quantum digital signatures [29]. In this paper they introduced the notion of a quantum one-way functions, that is a function whose input is a classical bit string k and whose output is a quantum state $|f_k\rangle$. The function made uses properties of quantum systems [13], namely that a quantum bit may be represented as a superposition of states $|\varphi\rangle = \alpha_o|0\rangle + \alpha_1|1\rangle$ and that the mapping $k \to |f_k\rangle$ is easy to compute and verify but it is impossible to reverse due to limits determined by quantum information theory. Holevo's theorem limits the amount of classical information that may be obtained from the quantum system. The digital scheme proposed is as follows; Alice chooses pairs of L-bit strings $\{k_0^i, k_1^i, \}, 1 \le i \le M$ where k_0^i is used to sign a message $b = 0$ and k_1^i used to sign a message with $b = 1$. These are used as the private keys in the protocol. Alice then prepares the states $\{|f_{k_0^i}\rangle, |f_{k_1^i}\rangle\}$ which will be used for Alice's public keys and used in the one way function. These public keys are accessible to all including potential forgers. For validation purposes Alice then sends a single-bit message b by sending the signed message $\left(b, k_b^1, k_b^2, \ldots, k_b^M\right)$ over an insecure classical channel. Each recipient, Bob and Charlie, are then able to perform the mapping $k_b^i \mapsto |f_{k_b^i}\rangle$ on the public keys via a swap test [30] and counts the number of incorrect keys. In practice this is done by both Bob and Charlie receiving two copies of the public key from Alice which means there are 4T copies of the public key in circulation. Verification is performed by each receiver verifying that everyone received the same public key $|f_{k_b^i}\rangle$. Each recipient first carries out a swap test between their two keys and then passes one copy to the other recipient who then carries out another swap test. If any of the keys fail the swap test then the protocol scheme is halted. The swap test involves checking that given the outputs $|f_k\rangle$ and $|f_{k'}\rangle$, is $k = k'$. To perform this swap test, an ancilla bit is prepared in the state $1/\sqrt{2}\left(|1\rangle + |0\rangle\right)$. The ancilla bit is used as the control bit in a Fredkin gate which acts on $|f_{k'}\rangle$ and $|f_k\rangle$. A Hadamard transform is then performed on the ancilla bit and measured. The swap test is passed if the result is $|0\rangle$ in the case where $|f_{k'}\rangle = |f_k\rangle$. If the result is $|1\rangle$ then the test fails, $k \neq k'$´, and happens with probability... If $\langle f_k | f_{k'}\rangle \le \delta$ then the result $|0\rangle$ will occur with a probability of at most $(1+\delta^2)/2$.

The above scheme set the foundations for quantum digital signatures schemes and can be seen as a quantum mechanical equivalent of the Lamport one-time signature discussed in section 5.5.1. However the paper did not elaborate about how such a

scheme could be practically implemented. It was not until 2006 that a paper by Anderson, Curty and Jex [31] proposed a practical way of implementing the a quantum signature scheme. The discussion and experiments in the following sections are based around such a system.

5.11 Security using coherent states in quantum information

The security of using coherent states in quantum information systems relies principally on the fact that it is impossible to perfectly distinguish between two non-orthogonally encoded coherent states. A coherent state with an amplitude α is an eigenstate of the annihilation operator $\hat{a}$. In the photon-number representation a coherent state may be defined as

$$|\alpha\rangle = \exp\left(-|\alpha|^2/2\right)\sum_{n=0}^{\infty}\frac{\alpha^n}{(n!)^{1/2}}|n\rangle \qquad \text{Equation (5.11)}$$

A coherent state occupies a particular area in phase space, due to the Heisenberg uncertainty principle such that given two coherent states $|+\alpha\rangle = e^{i\varphi}|\alpha\rangle$ and $|-\alpha\rangle = e^{i(\varphi+\pi)}|\alpha\rangle$ with $\varphi = 0$, the an overlap between the states is given by

$$f = e^{-2|\alpha|^2} \qquad \text{Equation (5.12)}$$

When the amplitude $|\alpha|^2$ becomes large the overlap approaches zero and the two states $|+\alpha\rangle$ and $|-\alpha\rangle$ are orthogonal. Alternatively, when $|\alpha|^2$ is small a quadrature amplitude measurement of the form $x = \left\langle e^{i\theta}\hat{a}^{\dagger} + e^{-i\theta}\hat{a}\right\rangle$ cannot unambiguously discriminate between the two states. For example a measurement of $|+\alpha\rangle$ may produce results that could have been produced if $|-\alpha\rangle$ was measured and vice versa. The implications of this can be understood by taking a sender Alice and receiver Bob who start communicate securely using coherent states in the presence of an eavesdropper. Alice can randomly prepare one of two non-orthogonal states and Bob guesses the state sent by measuring the amplitude of x. Assuming the transmitivity of the quantum channel $\eta = 1$ then Bob's probability of measuring incorrectly is given by

$$p_e = \frac{1}{2}\left(1-\sqrt{1-f^2}\right) \qquad \text{Equation (5.13)}$$

The error probability is directly related to the overlap of the states f and by Equation (5.12) also by the magnitude of $|\alpha|^2$.

Figure 5.6 shows the overlapping probability distribution for quantum states prepared as 0 and 1. The shape of the distribution and in particular the overlap can be exploited by Alice and Bob in post selection. For Bob's measurement result x which falls in the

centre region, the error probability of determining a 1 or 0 is high. On the left and right side of this region in the tails of the distribution, results can be verified as 1 or 0 with more certainty. For coherent states, Eve's and Bob's probability distributions of measurement outcomes x are independent which means that it is possible for Eve to obtain inconclusive results in which she is unable to assign a 1 or 0 while Bob is quite definite about the state. The mutual information shared between Alice and Eve I_{AE} depends only on Alice's selected amplitude $|\alpha|^2$ and is independent of the measurement results x of Eve and Bob. Alice and Bob are able to determine the error probability and their mutual information I_{AB} for each single event x after the measurement. For a given overlap f given by $|\alpha|^2$ Bob can establish a lower limit on his measurement result x such that $I_{AB} > I_{AE}$. Bob can select a threshold x_0 to eliminate inconclusive result that fall outside the range $x < |x_0|$. Owing to this fact, the shared knowledge between Alice and Bob about the selected events $x > |x_0|$ is larger than that shared between Alice and Eve, allowing a secret key to be distilled [32].

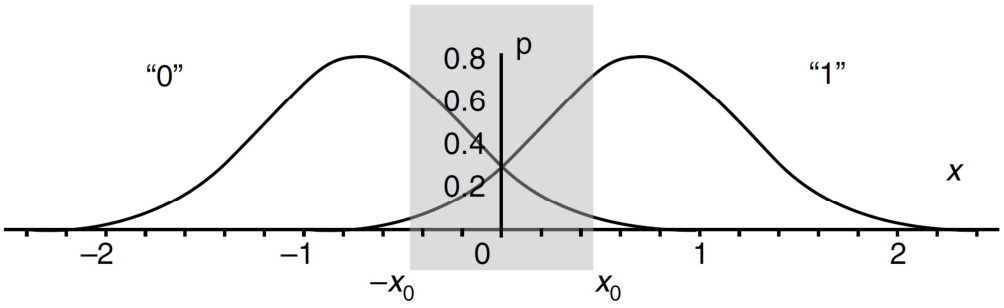

Figure 5.6. Probability distribution of measurements results x for two no-orthogonal signal state 1 and 0. The inconclusive results given by the shaded region can be removed in a post-selection procedure. The error probability is high in this region due to the large overlap of the probability distributions .. and $p(0)$ [32].

The previous paragraph describes the underlying principle behind the continuous variable QKD protocol briefly discussed in Chapter 2 and is also the principle behind the quantum digital signatures scheme in section 5.12. The above description only looked at using two non-orthogonal coherent states but the same ideas can be applied to the QDS protocol which used eight non-orthogonal states in the experimental demonstration. In essence by carefully controlling the overlap f by the choice of $|\alpha|^2$ Alice is able to ensure that the states cannot be determined unambiguously. The non-orthogonal states in the limit of large $|\alpha|^2$ become orthogonal enabling unauthorised parties to determine the state with complete certainty.

5.12 Quantum digital signatures

5.12.1 Comparison of quantum states for quantum digital signatures

The comparison of quantum systems is much more complication than its classical counterpart. It is not possible to measure all the observables of a system simultaneously and also the measurement value has a probabilistic outcome. The optimal way to compare the state of two unknown pure quantum systems is to check if their combined state is symmetric or anti-symmetric [33], [34]. Experimentally this can be done using a symmetric 50:50 beam splitter [35]. Two photons incident on the beam splitter will exit via different ports if they are in the anti-symmetric polarisation state and exit in the same port if they are in the symmetric polarisation state. If two quantum states have been prepared in the same initial state then their combined state is also symmetric. This means that finding the state in an anti-symmetric state is a definite indication that the two states were different. The choice of coherent states allows better than optimal success probability of determining if two states are equal. In the case of two general pure quantum states $|\varphi\rangle$ and $|\phi\rangle$, the success probability of determining if they are equal for the universal comparison strategy is the probability of them being an anti-symmetric state is given by

$$P_{asym} = \frac{1}{2}\left(1 - \left|\langle\phi|\varphi\rangle\right|^2\right) \qquad \text{Equation (5.14)}$$

For coherent states this becomes

$$P_{asym} = \frac{1}{2}\left(1 - e^{-|\alpha-\beta|^2}\right) \qquad \text{Equation (5.15)}$$

The success probability for the coherent state comparison is given by

$$P_{asym} = 1 - e^{-\frac{1}{2}|\alpha-\beta|^2} \qquad \text{Equation (5.16)}$$

which is larger than the universal comparison method [31].

Figure 5.7(a) shows how two coherent states of light [36] mix on a beamsplitter [37]. A coherent state is the quantum mechanical equivalent of a classical monochromatic electromagnetic wave. The equivalence between a light wave and a harmonic oscillator allows properties of the quantised harmonic oscillator to be applied to the quantised electromagnetic field states [38]. In mathematical terms it can be stated that $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$, where $\hat{a}$ is the annihilation operator for the relevant electromagnetic field mode. The input states to the beamsplitter are $|\alpha\rangle$ and $|\beta\rangle$ and the outputs given by $1/\sqrt{2}\,|(\alpha-\beta)\rangle$ and $1/\sqrt{2}\,|(\alpha+\beta)\rangle$. It is possible to see that if $\alpha = \beta$ then

$1/\sqrt{2}\left|(\alpha-\beta)\right\rangle = 1/\sqrt{2}\left|(\beta-\beta)\right\rangle = \left|0\right\rangle$ which is the vacuum state, and no light exits through that port. This simple operation forms the basis of the signature verification protocol. Figure 5.7(b) shows a schematic representation of the signature comparison system employed by Bob and Charlie [39]. At each receiver the signature from Alice is split into two equal amplitude components and one of these is shared with the other receiver who performs the same action on their copy of the signature. The retained component of the signature is then mixed on a beamsplitter with the component transmitted from the other receiver. It can be seen from Figure 5.7(b) that if the two components are the same then the original signature will be recovered through one port of the beamsplitter and a vacuum state $\left|0\right\rangle$ will be generated at the other. In order to detect any attempts by Alice to send differing signatures to Bob and Charlie only requires detection of any non-zero number of photons at the relevant beamsplitter ports.

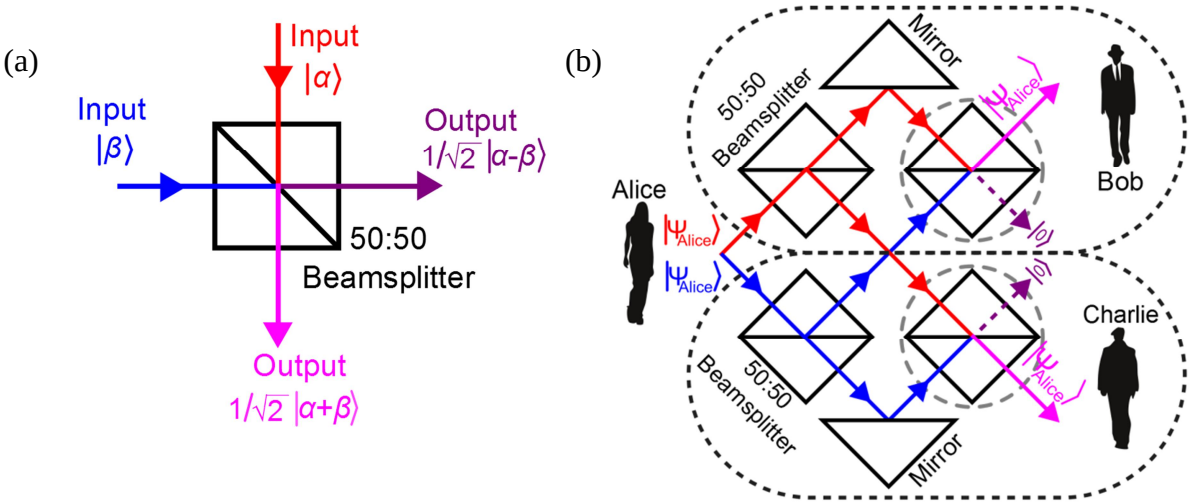

Figure 5.7. Field mixing on a balanced splitting ratio cube. The states $\left|\alpha\right\rangle$ and $\left|\beta\right\rangle$ are coherent states. (b) Public key distribution in the case where Alice (the sender) is not trusted. Bob and Charlie (the receivers) separate half of the key from Alice and send it to the other party where it is compared on a beamsplitter with the other party's key half.

The QDS protocol is implemented as follows, Alice randomly selects a series of phase encodings from the set $\{2\pi k/N, k=0,1,\ldots,N-1\}$ where N is the number of possible phase encodings and k is an integer in the range 0 to $N-1$. Alice sends a series of phase encoded coherent states $\rho_{0,l}$ and $\rho_{1,l}$ (analogous to the classical public key) to receivers Bob and Charlie. The $\rho_{0,l}$ phase encoding are those used sign a binary "0" at

position l in the message (where l is an integer of less than or equal to the message length, M) and the $\rho_{1,l}$ phase encodings are those used sign a binary "1" at position l. Bob and Charlie pass the complete series of encoded states ρ_0 and ρ_1 through the comparison system multiport of Figure 5.7(b) to verify that they both received the same phase encoded states. If the signature states were identical coherent states then the multiport will preserve them otherwise the overall state shared by Bob and Charlie will become symmetrised which prevents repudiation by Alice. Bob and Charlie store their phase encoded states in quantum memory [40] until they need them. To sign a message Alice then sends a message and the classical description of the corresponding state (analogous to the classical private key) to Bob and Charlie. Bob and Charlie check the states against those stored in their memory by measurement. Bob for example can check the classical description of the key states against those stored in his quantum memory by generating coherent states according to Alice's description and individually interferes them with the corresponding states in his memory. He then checks whether the number of photodetection events at the signal null-port, shown in Figure 5.9, is smaller than $s_a L$, called the authentication threshold. If the message passes authentication Bob can then prove to Charlie that the signed message came from Alice by forwarding the message to Charlie and the classical description of the signature states he received from Alice. In order to verify that a signed message forward by Bob, Charlie follows the same procedure just described for Bob but with a modified threshold $S_v > S_a$ called the verification threshold. A difference g between the two thresholds ensures that Alice cannot make one of them accept while the other rejects a message except with increasing small probability as g increases. The quantum digital scheme can be thought of as a quantum version of the Lamport public key scheme described in section 5.5.1

The choice of mean photon number per pulse $|\alpha|^2$ for the coherent states emitted by Alice to each party depends on the number of possible phase encodings N in her alphabet and the signature length M. A greater number of coherent states per signed bit increases security for a given $|\alpha|^2$. Figure 5.8 shows how the information on each encoded laser pulse available to a malicious party, given by the von Neumann entropy [41] $S(\rho_{\text{single}})$, for two receivers ($T = 2$) varies with increasing $|\alpha|^2$. For each position in the key string of length M there are N possible encodings therefore there are N^M possible states. The accessible information which can be obtained on the state in a single key position is bounded by

$$I_{acc} \le \chi\left(\rho_{key}\right) = S\left(\rho_{key}\right) - \sum_n p_n S\left(\rho_n\right) \qquad \text{Equation (5.17)}$$

where $S\left(\rho_{key}\right)$ is the Von Neumann entropy of ρ_{key}. It is necessary to ensure that the information about the whole signature known by Alice far exceeds that which is accessible to a malicious party, $M \cdot \log_2\left(N\right) >> M \cdot T \cdot S\left(\rho_{Single}\right)$. Figure 5.8, shows that values of $|\alpha|^2$ must be chosen so that the corresponding values of $T \cdot S\left(\rho_{\text{single}}\right)$ are far below the corresponding dashed asymptote.

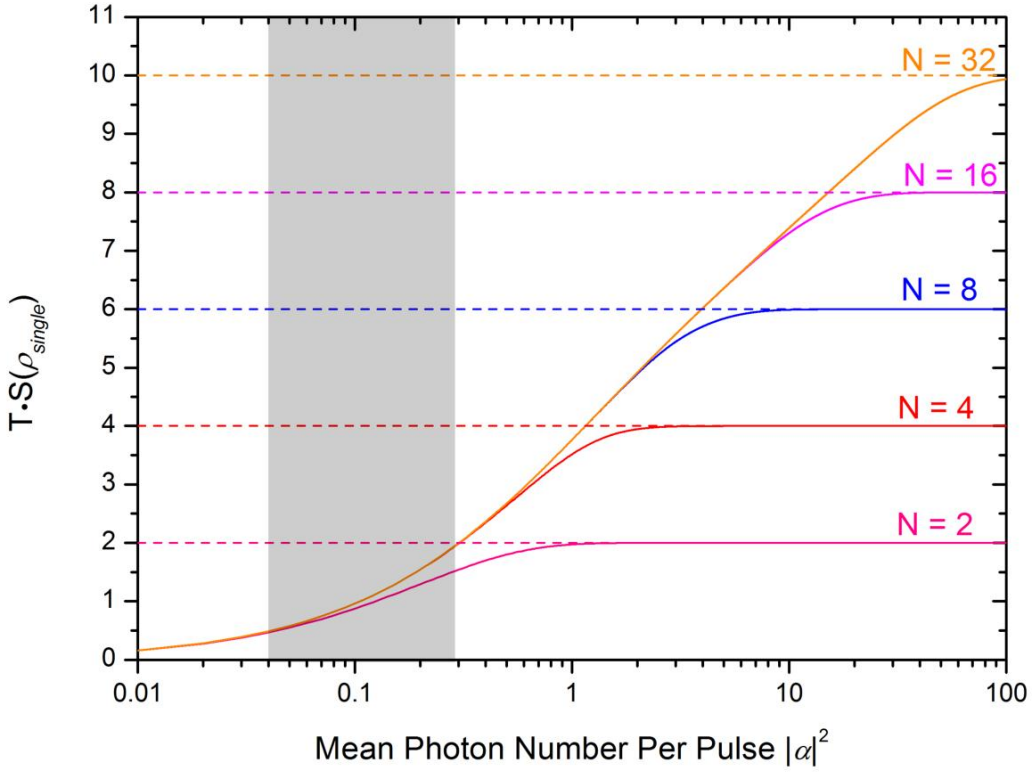

Figure 5.8. The von Neumann entropy $S\left(\rho_{Single}\right)$ for two receivers (Charlie and Bob, therefore $T = 2$) as a function of the mean photon number $|\alpha|^2$ for number of phase encodings N equal to 2, 4, 8, 16 and 32. The greyed region indicates the range of $|\alpha|^2$ values used in the experiment. The asymptotic value of the entropy increases with the number of phase encodings N, indicating that it is possible to use higher $|\alpha|^2$ values for greater values of N.

5.12.2 QDS Experimental system

The signature verification scheme was experimentally implemented in optical fibre as shown in Figure 5.9. The system has many design and component similarities to the quantum key distribution system described in Chapter 4 in regard to experimental setup

and data acquisition and processing. The most common feature to both systems is the use of asymmetric unbalanced Mach Zehnder interferometers for encoding information on pulses of light. The quantum digital signatures (QDS) system was assembled from polarisation maintaining (PM) fibre which supports a single-mode at a wavelength of 850 nm. PM fiber ensures that random fluctuations in the polarisation of light guided in the fibre which could degrade the interferometric visibility are removed [42].

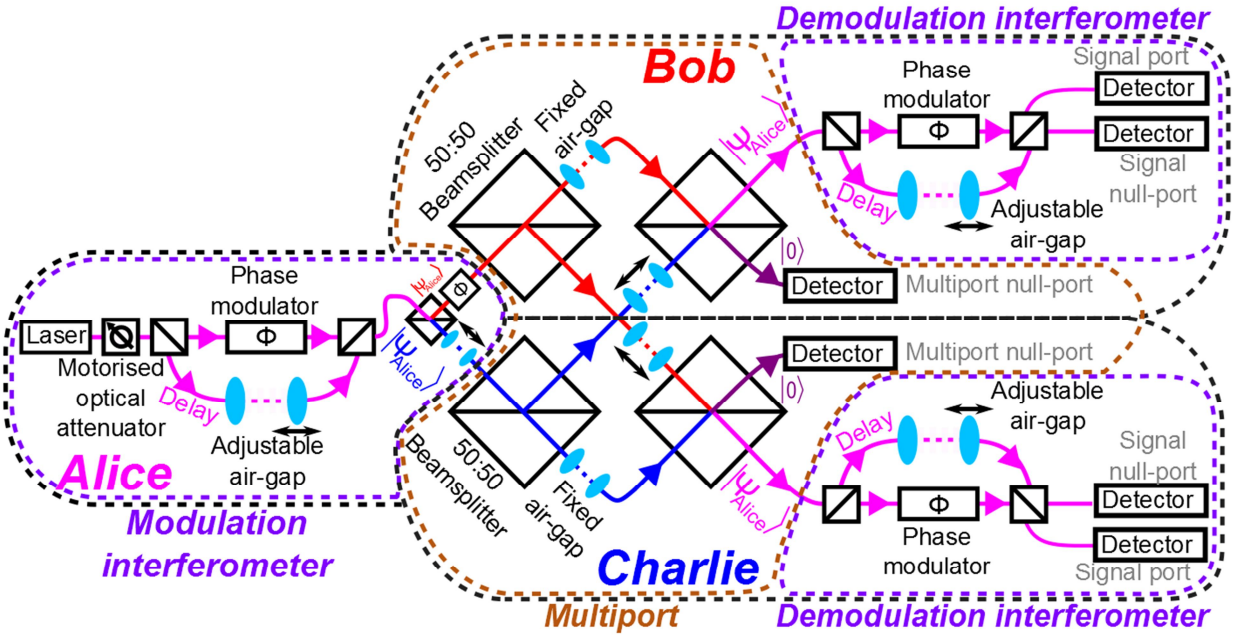

Figure 5.9. A schematic of the experimental demonstration of quantum digital signatures. The laser used is a vertical cavity surface emitting laser (VCSEL) and the detector is a single-photon avalanche diode. The addition of a phase modulator in the fibre length between the 50:50 beamsplitter in Alice's and Bob's entry point to the multiport allows to test scenarios where Alice attempts to cheat by sending different phase states. The motorised optical attenuator allows Alice to vary the amplitude of her phase encoded pulses.

5.12.2.1 Laser source characterisation

The spectral profile of the vertical cavity surface emitting laser (VCSEL) which provides the multiphoton pulses is shown in Figure 5.10 showing a central wavelength of 849.8 nm and a full-width half-maximum (FWHM) of 0.23 nm.

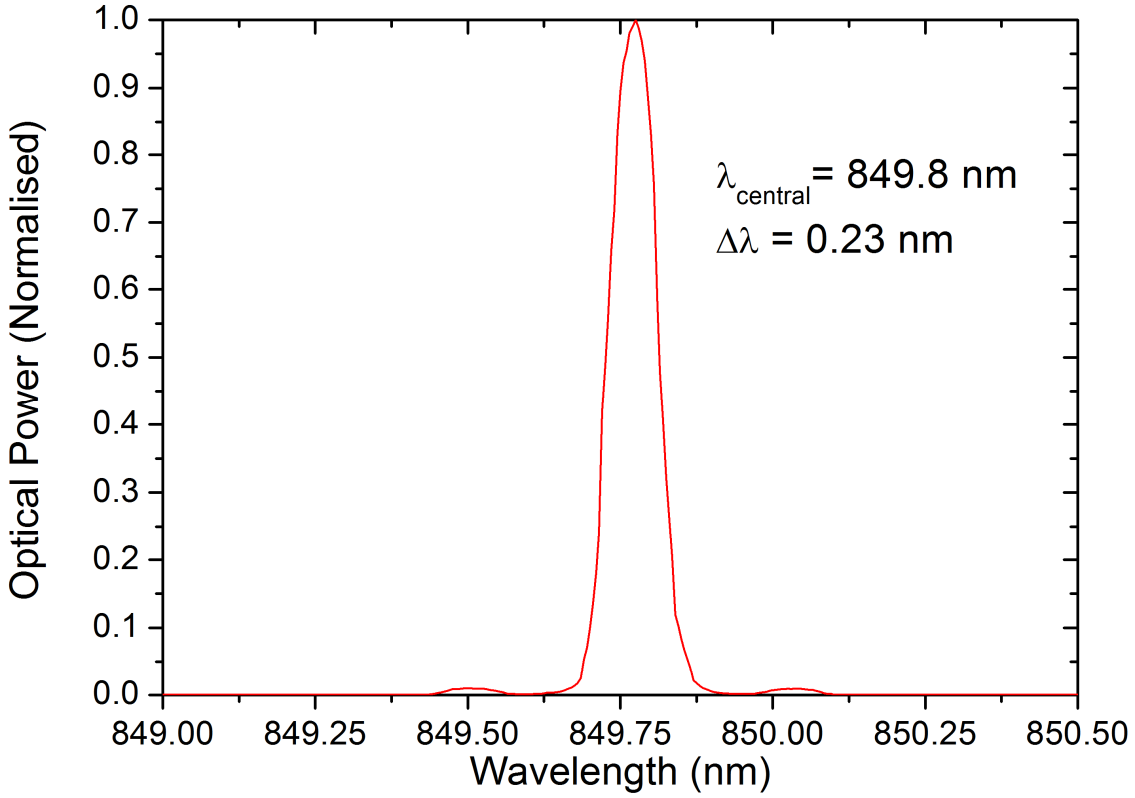

Figure 5.10. The spectra of the vertical cavity surface emitting laser profile under operating conditions used in these experiments, taken using an optical spectrum analyser with a resolution of 0.1 nm. The quoted FWHM was obtained by fitting a Gaussian curve to the recorded spectrum. The central wavelength was measured to be 849.8 nm having a FWHM of 0.23 nm.

The relation between interferometric fringe visibility V and the linewidth $\Delta\nu$ of the source is given by

$$V = \exp\left[\frac{-(\pi\tau\Delta\nu)}{4\ln 2}\right] \qquad \text{Equation (5.18)}$$

where τ is the temporal delay between the interfering light. This implies that a narrower linewidth source gives improved visibility although misalignment of the stress members in PM fibre can also degrade this value.

The temporal profile of the VCSEL is shown in Figure 5.11 and has a FWHM of 0.924 ns.

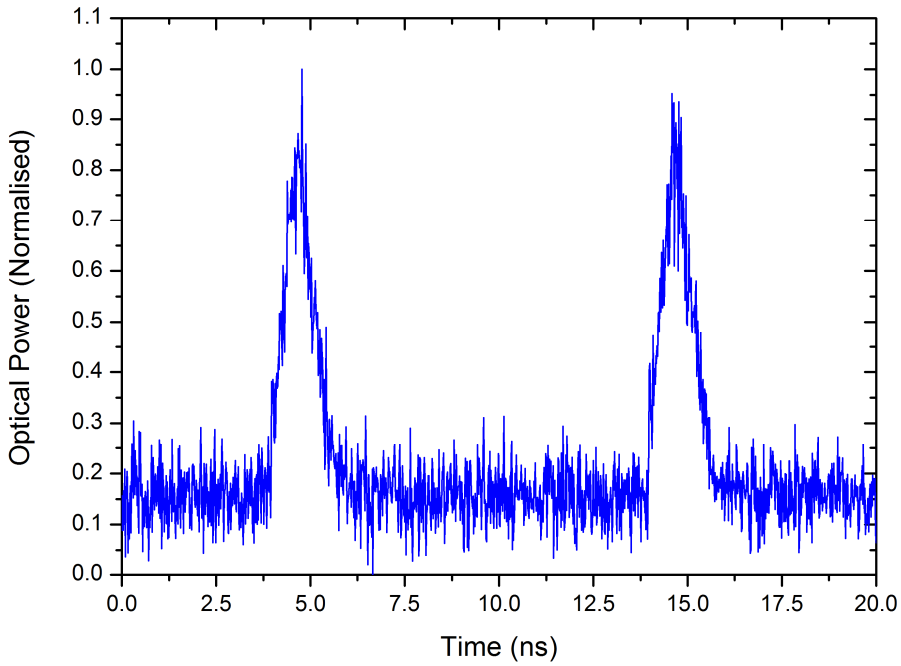

Figure 5.11. The temporal profile of the VCSEL under operating conditions, taken using a 12 GHz InGaAs Schottky amplified photoreceiver with a 30 ps risetime. The FWHM was measured to be 0.924 ns.

The VCSEL was pulsed using a high speed laser driver board (MAXIM3996) shown in Figure 5.12 and is designed for fiber optic local area network (LAN) transmitters [43].

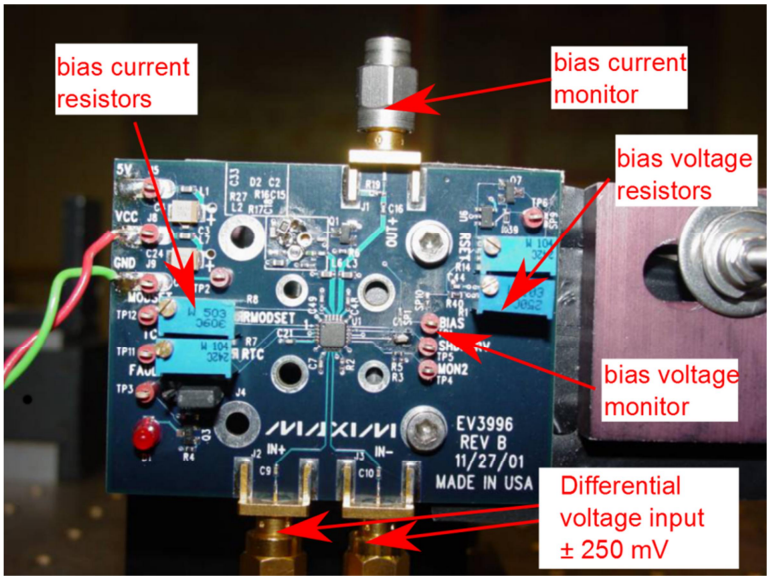

Figure 5.12. MAXIM driver board for the VCSEL.

This board has an automatic power control that adjusts the laser bias current to maintain the optical power constant regardless of changes in the operating temperature however the laser is still maintained at a constant temperature of 15 ºC (± 0.1 ºC) using custom

designed in-house controller. An Agilent 81134A pulse pattern generator (PPG) provided the ±250 mV differential input voltage to the driver board. Variable resistors on the board allow the amplitude of the modulation current to be modified until an optical pulse with the shortest temporal duration as in Figure 5.11 to be obtained.

Figure 5.13 demonstrates that by operating at a pulse repetition frequency of 100 MHz avoids temporal intersymbol interference when using high detection efficiency commercial thick junction detectors. Although thin-junction Si-SPADs have superior timing resolution compared to thin junction ones, by operating at a clock rate of 100 MHz means that with regard to bit rate it is more beneficial to use high detection efficiency detectors. A wavelength of 850 nm was chosen to ensure good compatibility with comparatively mature silicon single-photon avalanche diodes (Si-SPADs) which have a detection efficiency of ~40% at this wavelength [44]. SPADs were selected as the detectors as the losses of the system mean that the pulses transmitted by Alice are in the single-photon regime at the detectors. The losses of Charlie's and Bob's demodulation interferometers are ~6 dB each. The loss of the multiport signal port in Charles's and Bob's multiport are 6 dB and 7.6 dB respectively.

The current lack of low cost and easy to use quantum memory which can allow the long term storage of photons [45], [46] requires the experimental system to directly measure the phase of the photon after it has left the multiport. To achieve this, a phase reference pulse is required. The system time multiplexes a phase reference pulse between successive 10 ns separated signal pulses using an asymmetric double Mach-Zehnder approach as demonstrated in many quantum key distribution systems employing phase encoding [47]. The same approach is adopted in Chapter 4 which used Mach-Zehnder interferometers for encoding phase in a quantum key distribution system. In an ideal QDS system, the receivers would use their paths with air-gaps (OZ Optics ODL-200) to delay only the signal pulse so that it recombines with the corresponding reference, revealing the phase encoding. However, in this current system there will be photons which take non-interfering paths in sender and receiver (i.e. both short paths or both delayed paths) contributing nothing to the signature and theses are software gated from the photon arrival times recorded using the free-running SPADs. Figure 5.13 shows the non-interfering pulses together with a constructive (maximum) and destructive (minimum) interferences pulses.

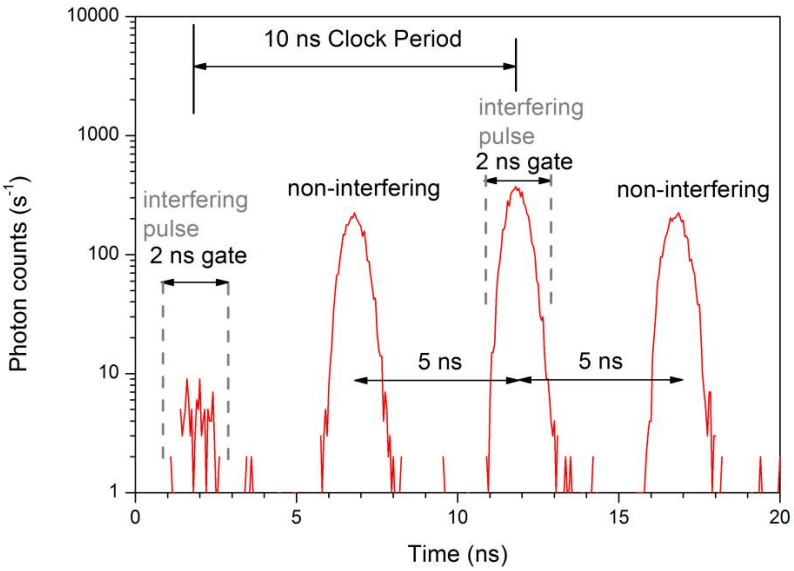

Figure 5.13. System instrumental response from the QDS system. Two interfering peaks are visible, one for constructive and one for destructive interference along with the two non-interfering peaks. Also shown is the position and width of the gate for calculating the encoding error and bit rate.

In post-processing, the time gating software opens a window of duration 2 ns centered on the expected arrival time of a pulse and disregards events which occur outside of this window. The events which lie outside of this window are still recorded by the acquisition electronics. In a full system with quantum memory there would be no need for the asymmetric double Mach-Zehnder interferometers and the phase encoded photons would be stored in quantum memory at the output of the comparison stage, making the raw count-rate in the experiments closer to that which would be obtained if quantum memory was available.

Environmental fluctuations can destabilise the Mach-Zehnder interferometers and result in large phase encoding errors. Each variable air-gap in the multiport and demodulation interferometers contains a piezoelectric brick positioned in the vernier mechanism which is connected to a voltage generator under computer control. Alice, Bob and Charlie can ensure that each of their interferometers is correctly aligned in relation to their phase by Alice sending a prearranged sequence of phase encoded bits. Alice and each receiver then perform a correlation between the sent and received sequence and adjusts the voltage on the piezoelectric brick until a maximum is obtained in their correlation. A similar procedure is used in Chapter 4 for tuning the interferometers in the QKD system and is described in more detail there.

To generate a series of 8 equally spaced phase encodings in the range $0\ldots 2\pi$ required that the pulse pattern generator (PPG) was capable of generating the required number of states. A similar approach was adopted here as in Chapter 4 for the generation of 4 phase encodings for the BB84 protocol. A schematic of the approach adopted here is shown in Figure 5.14. An Agilent 81110A dual output pulse pattern generator was capable of internally combining its two outputs resulting in a four step data pattern of levels 0, 3, 6 and 9 volts. This output was then combined with the output of an Agilent 81134A PPG with a voltage step of 1.5 volts. This second PPG although capable of operating at higher clock speeds was only capable of outputting 2 volts peak-to-peak. The final combined output resulted in voltage levels of 0, 1.5, 3, 4.5, 6, 7.5, 9, and 10.5 volts. The increment of 1.5 volts between each state ensured an equal spacing between the generated states due to the V_π of 6 volts for the phase modulator crystal. The electrical driving signal which is applied to the phase modulator is shown in Figure 5.15. The electrical signal shows some electrical ringing especially at transitions from one state to the next which could result in large phase encoding errors but this effect can be minimised by pulsing the laser at occasions when the electrical signal is for each state is constant as shown in Figure 5.15. The phase encoding error which can be attributed to the phase jitter in the polarisation modulators can be given by

$$Error_{phase} = \frac{1}{\Delta\phi}\int_{-\frac{\Delta\phi}{2}}^{+\frac{\Delta\phi}{2}} \frac{1-\cos\phi}{2} d\phi \qquad \text{Equation (5.19)}$$

where $\Delta\phi$ is the variation in phase caused by the modulator [48]. The amplitude jitter of the electrical signal for the phase modulator is 200 mV which corresponds to a maximum error in the phase of 0.1 radians as the voltage required for a phase shift of π radians is 6 volts. $Error_{phase}$ is ~0.02%.

The QDS system described here requires the timing information from 6 detectors, two for events on Bob's and Charlie's multiport null-ports and four to record events on their signal port and signal null-ports. The dual input GT658 time interval analyser [49] (TIA) described in Chapter 2, was used to record events on the two multiport null-port arms and PicoQuant's HydraHarp quad input TIA [50] was used to record events on Bob's and Charlie's demodulation interferometers. As these TIAs have independent clocks it is necessary to ensure that the time tags recorded on each device were correctly synchronized. A 10 MHz Rubidium (Rb) (Novatech 2960 AR) frequency standard was used as the master clock for the system and used for the reference signal for the internal

phased locked loop (PLL) in each pulse pattern generator (PPG). Phase locked loops are a control system that generates an output voltage whose phase is regulated by the phase of an input reference signal [51]. The Rb clock had a 1 pulse per second output (1 PPS) that was used as the external arming input for the GT658 and the input reference for the HydraHarp. This 1 PPS signal can be used to synchronise the internal clocks in the TIAs and compensate for any electrical timing delay to ensure that histograms obtained on both devices when timing events are derived from the same signal source occur at the same bin/time position.

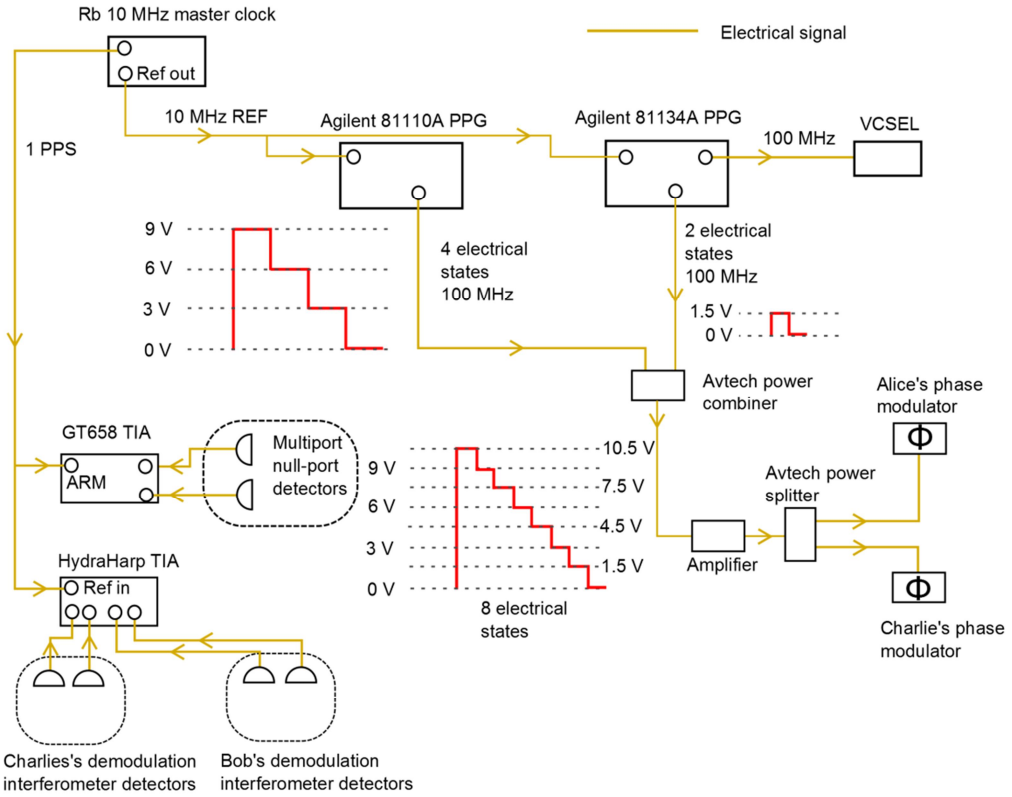

Figure 5.14. Electrical schematic for the QDS system. The Agilent 81110A PPG produces a four level step pattern of 0, 3, 6 and 9 V which is then combined with a 0 and 1.5 V step pattern from the Agilent 81134A PPG to create the required voltage pattern for encoding 8 states. The signal is amplified and then split and sent to Alice's and Charlie's phase modulator. The one pulse-per-second (PPS) output from the 10 MHz Rb master clock is used to synchronise the independent clocks of the GT658 and HydraHarp TIA cards. The HydraHarp TIA records timing events from Bob's and Charlie's demodulation interferometers while the GT658 TIA records the multiport null-port events.

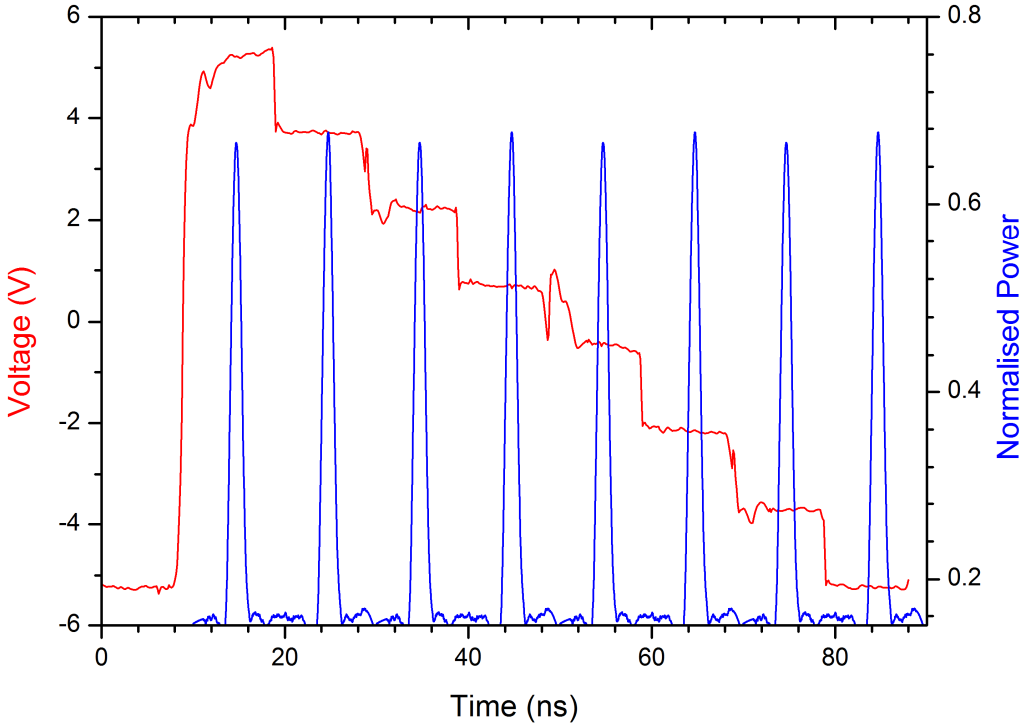

Figure 5.15. Electrical driving signal for the generation of 8 phase encodings with the temporal response of the VCSEL superimposed (temporal response shows two periods which was then simulated for the remained 6 pulses)

The presence of a phase modulator in the section of fibre prior to either Bob or Charlie allows the investigation of the case where Alice sends different signatures to different recipients. The air-gap in the other arm allows the transmission losses to be balanced between each arm so that the same $|\alpha|^2$ value is launched to each recipient and permits compensation for small path-length differences between the two launch arms. $|\alpha|^2$ is defined after the phase modulator/air-gap before entry into the multiport. $|\alpha|^2$ is set by a computer controlled motorised attenuator which is accurate to within 1% of the calibrated value. The measured pulse-to-pulse variance in the amplitude of the laser was less than 3%. An exact measurement was noise limited by the detector used and a deconvolution method had to be used to estimate the worst case variance.

5.12.3 Experimental results

Figure 5.16 shows the experimental results obtained from Charlie in the system using eight equally spaced phase encodings ($N = 8$) and an honest Alice sending the same signature to both Bob and Charlie. For these measurements the phase modulator in the Alice to Bob arm was deactivated. The dashed lines represent the predictions for the

quantities made by a theoretical model and the data points are actual experimentally recorded values. The signal port raw rate is given by

$$Signal_{raw} = \nu \cdot \eta \cdot \mu \cdot \alpha_{receiver} \cdot \left(\frac{V+1}{2} \right) + R_{dark} \qquad \text{Equation (5.20)}$$

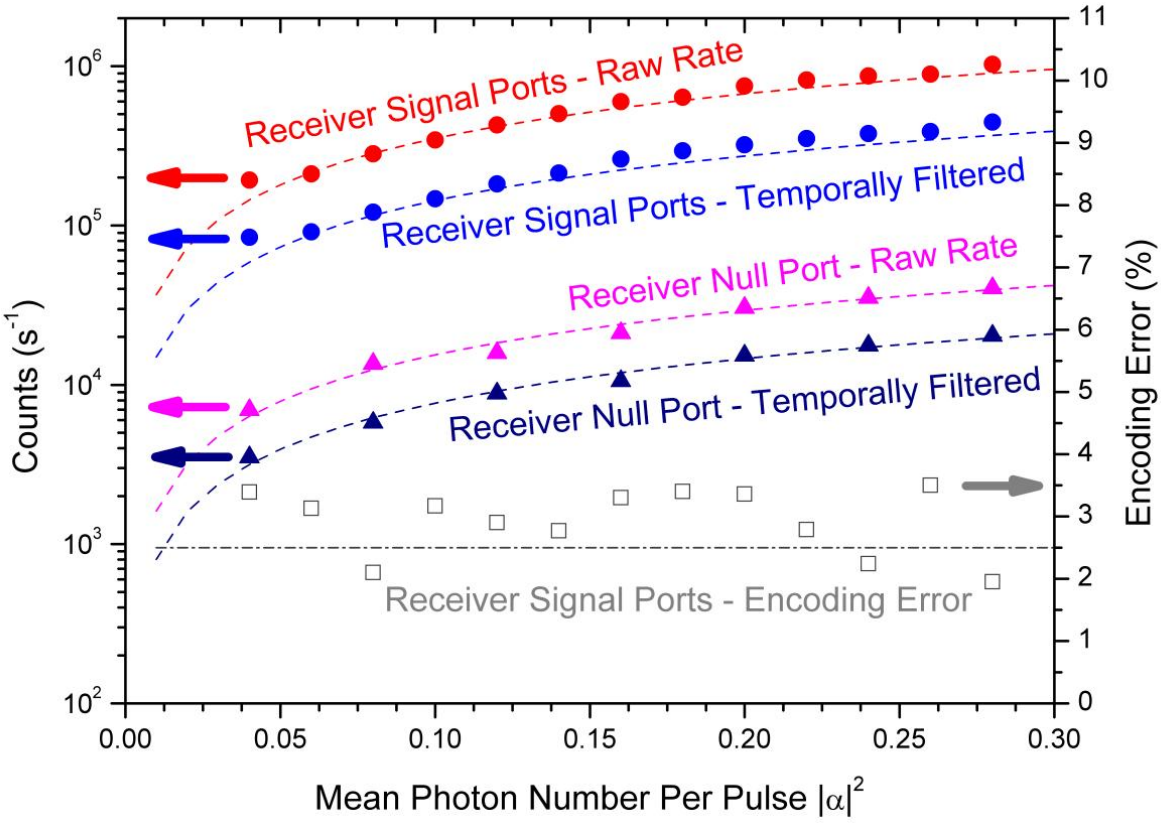

Figure 5.16. Experimental system results for one receiver, in this case Charlie, with eight equally spaced phase encodings. The system clock rate was 100 MHz. Data points represent actual experimental results while dashed lines are theoretical predictions. The raw count rate is the detector click rate summed over both of Charlie's signal SPADs after the asymmetric double Mach-Zehnder interferometers, the time gated count rate is the raw count rate after temporal filtering using a 2 ns duration window centred on the expected arrival time to reduce the effects of non-photon generated events, intersymbol interference and non-interfering photons. The encoding error is the number of pulses incorrectly phase demodulated by Charlie over the total number of pulses he received.

where ν is the clock frequency, η is the detector efficiency, $\alpha_{receiver}$ is the fractional loss of the receiver V is the interferometric visibility and R_{dark} is the dark count rate of the detector. The null port raw rate is given by

$$Null_{Raw} = \nu \cdot \eta \cdot \mu \cdot \alpha_{receiver} \left(\frac{1-V}{2} \right) + R_{dark} \qquad \text{Equation (5.21)}$$

The above equation assumes a 96% fringe visibility for both the comparison system and the combined encoding/decoding asymmetric Mach-Zehnder interferometers. As the mean photon number per pulse launched by Alice into the comparison system increases, so the count rate at the detectors increases. The multiport null-port count rates are significantly lower than those at the signal port but are non-zero. The counts in this port are primarily due to the interferometric fringe visibility of the multiport (although dark count events at the detectors do make a small contribution) and can be predicted, as denoted by the dashed lines. This null port rate sets a baseline for the system operating with an honest Alice. The temporally filtered rates are calculated by multiplying Equation (5.20) and Equation (5.21) by

$$I_{system}(\Delta T) = \frac{1}{\int_0^{2\frac{1}{\nu}} P_{arrival} dt} \cdot \int_{t_{\max}-\Delta T/2}^{t_{\max}+\Delta T/2} P_{arrival}(t)\, dt \qquad \text{Equation (5.22)}$$

where $t_{\max}$ is defined in Figure 5.13. This essentially treats the four possible paths that a photon can take though a cascaded Mach-Zehnder as a stochastic process whose probability is affected by the differing attenuation in each path. $P_{arrival}(t)$ is generated by fitting a piecewise Gaussian-exponential function to the detector instrumental response and recreating a histogram of the possible paths a photon takes through the system, scaling the heights according to the loss occurred in each path as shown in Figure 5.13. The recorded arrival time of a photon on a TIA depends on the particular path taken and also on the timing jitter of the detector. Figure 5.13 shows two gating windows of 2 ns duration (ΔT) which are centered on the maximum probability of the arrival time for interfering peaks. Only those counts which fall inside the gating windows are included in the temporally filtered rate and $I_{system}(\Delta T)$ was calculated to be ~0.4 of the raw count rate, using Equation (5.22). The encoding error is defined as the number of temporally filtered pulses detected by a receiver at his signal null-port, divided by the temporally filtered total number of pulses recorded by that receiver. The encoding error rate is constant within experimental fluctuations across the range of experimentally examined $|\alpha|^2$ values for as the effects of intersymbol interference and dark count events in the detectors (dark counts) are negligible. The detectors have a mean dark count rate across all six detectors (three each in Bob and Charlie) of 320

counts per second and the probability of intersymbol interference for each detector is 3×10^{-8}. The contribution to the encoding error due the phase encoding error, the interferometric visibility, the dark count rate and temporal intersymbol interference is given by

$$Error_{encoding} = Error_{phase} + Error_{decoding} + Error_{dark} + Error_{jitter} \qquad \text{Equation (5.23)}$$

The terms $Error_{dark}$ and $Error_{jitter}$ summed contribution to the encoding error for the QDS system is less 0.01%. The term $Error_{Decoding}$ is due to the interferometric visibility of the interferometer and can be given by

$$Error_{decoding} = \frac{1-\vartheta_{Visibility}}{2} \qquad \text{Equation (5.24)}$$

where $\vartheta_{Visibility}$ is the classical visibility of the interferometer. For a fringe visibility of 96% $Error_{decoding}$ is 2%.

5.12.4 Cheating scenarios in QDS: Forgery by Bob

Assuming Bob to be the forger, Charlie should be able to detect a mismatch between Alice's choose phase encoding in a signature state and Bob's best average guess if the system is to be immune to forgery. This mismatch results in a higher probability for a photodetection event on Charlie's signal null-port when he measures the state using a phase different from that in which it was encode in. This scenario was experimentally tested by examining the encoding error at Charlie if he measures using a phase difference from that defined by Alice, shown in Figure 5.17 and quantifies the effects of a mismatch between the encodings in true and forged signatures. The encoding error used here is defined as the fraction of encoded photons sent by Alice which are incorrectly phase modulated by Bob. The symmetry of the phase encoding/decoding process is evident by observing the diagonal elements in Figure 5.17 and the matrix elements in Table 5.1. The off diagonal elements indicate the case where Charlie measured incorrectly and clearly show that if Charlie measures using a different phase form that sent by Alice he observes an increase in his encoding error when Bob attempts to forge a message. A greater difference between the probabilities of null-port events for differing and identical phases reduces the required key length for a desired level of security.

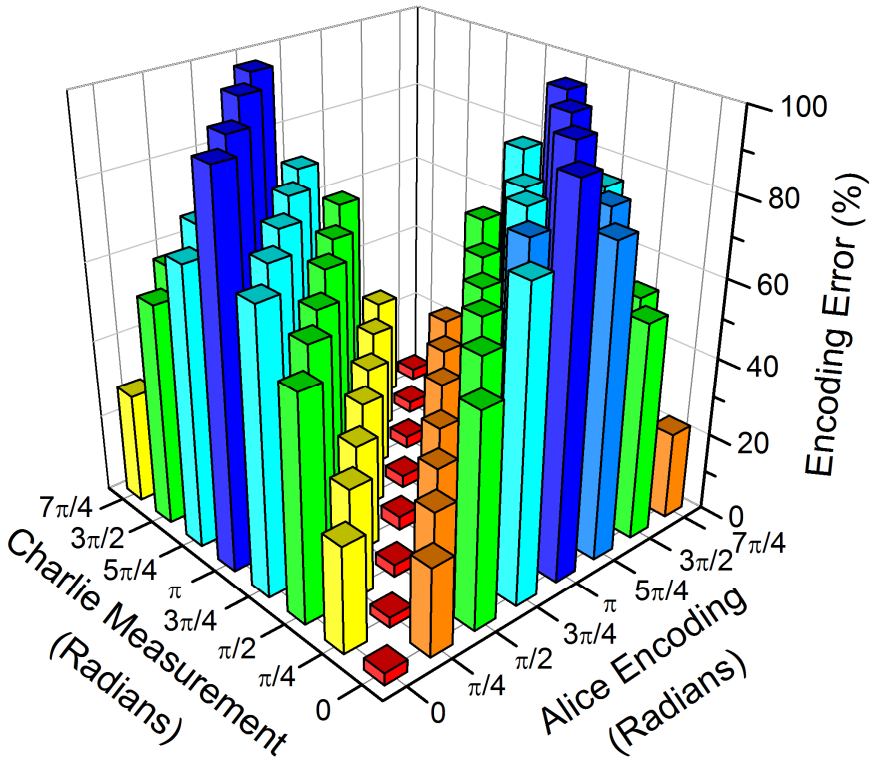

Figure 5.17. The variance in encoding error (expressed as a percentage) for Charlie when he measures using the same and different phases from that sent by Alice. The result shows that Charlie can detect an increase in his encoding error % when Bob attempts to forge a message. The above matrix allows the probability of cheating in a passive attack to be evaluated.

Charlie's phase decoding (radians)

Alice phase encoding (radians)	0	$\pi/4$	$\pi/2$	$3\pi/4$	π	$5\pi/4$	$3\pi/2$	$3\pi/2$
0	3	22.4	53.4	77.2	95	78.2	55.1	22.1
$\pi/4$	26.8	2.6	23.3	55.8	78.3	96.1	78.1	52.5
$\pi/2$	56.2	28.3	3.1	22.5	55.7	77.8	95.7	75.5
$3\pi/4$	70.8	57.3	27.5	3.5	21.9	53.8	74.9	94.9
π	96	71.2	56.3	27.7	3	23.5	53.4	77.5
$5\pi/4$	70.5	95.7	71.1	57.6	27	3.1	23.1	55.4
$3\pi/2$	56.3	71.7	97.9	71.6	57.1	27.5	2.8	22.5
$7\pi/4$	28	57.2	71.1	97.6	71.3	58.6	27	2.9

Table 5.1. The variance in encoding error (expressed as a percentage) for Charlie measuring using the same and different phases from that sent by Alice.

5.12.5 Cheating by Alice

The QDS system can be tested against the case were Alice attempts potentially the simplest form of cheating on the system and sends slightly different signatures to Bob and Charlie using the phase modulator in the fibre connecting Alice to Bob in order to change the phase encoding of certain pulses in the signature sequence. The system was setup to change the phase of two pulses in every sixteen by a fixed phase and the count rate at the multiport null port and the error rate at Charlie were monitored. The results for the raw count rate at the multiport null port can be seen in Figure 5.18. It can be observed from Figure 5.18 that as Alice increases the magnitude of the phase difference between the states, the count rate at Charlie's null port increases as expected and this simple cheating strategy by Alice is relatively easy to detect.

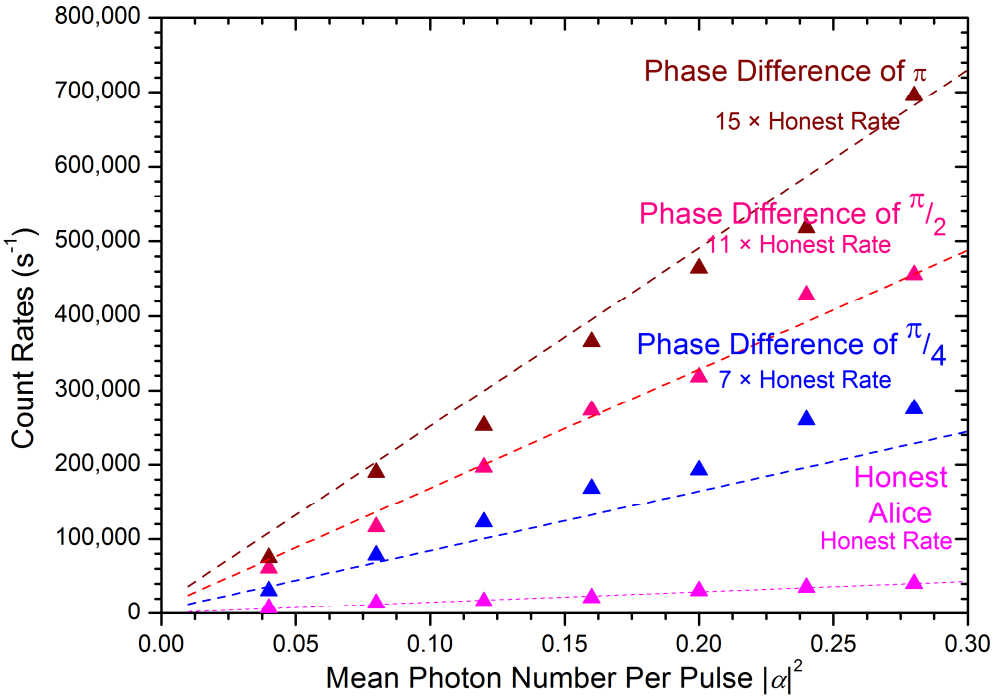

Figure 5.18. Alice cheats in the simplest way and tries to send different signatures to Bob and Charlie. She alters the phase encoding of two pulses in every sixteen by a fixed amount. The "Honest rate" is the observed null port count rate when Alice is not cheating and sends the same signature to Bob and Charlie. It can be observed that as Alice makes progressively greater changes to the phase encodings sent to one party, the count rate at the null port increases. The dashed lines represent the predicted count rate using Equation (5.21) and the cosine phase sensitivity of the interferometer.

5.12.6 Security Overview

The QDS system is considered secure if it demonstrates security against forging, repudiation and is robust. Security against forging means that the probability of

producing a private message m which was not sent from Alice, and passes verification by all other recipients decays exponentially quickly with the length L of the quantum digital signature. Security against repudiation entails that for any malicious activity on the part of Alice, the probability of a message failing verification with one recipient once it has already passed authentication with the other decays exponentially fast in terms of L. The QDS system is considered robust if when all parties are honest then a message will be authenticated and verified except with a probability which decays exponentially quickly in terms of L.

5.12.6.1 Forging quantum digital signatures

In the scenario where either recipient is dishonest (Charlie or Bob) there are two possible forging strategies available to them. In the active attack the malicious party has the ability to alter the states he forwards to the other party within the multiport which enables him to maximise his cheating probabilities later. In the passive attack Bob does not interfere throughout the quantum signature but attempts to cheat by inspecting his copy of the quantum signature. If one assumes that Bob is the potential forger then in the passive attack the probability of Bob generating a photodetection event with Charlie per individual quantum signature element is given by

$$p_{forgery} = \min_{\{\{\Pi_\phi\}\}} \frac{1}{N} \sum_{\phi} \sum_{\theta} \mathrm{Tr}\left(\Pi_\phi \rho^\theta\right) c_{\phi,\theta} \qquad \text{Equation (5.25)}$$

where $\mathrm{Tr}\left(\Pi_\phi \rho^\theta\right)$ is the probability that Bob measures and thus later declares the angle ϕ if the state he measured was encoded with the angle θ, ρ^θ is the coherent state sent by Alice with a chosen phase θ, $c_{\phi,\theta}$ is the probability of Charlie registering a photodetection event in his signal null-port if the state he had in his memory was encoded with θ and Bob declared ϕ. Π_ϕ are operators which describe the measurement performed by Bob on the signature copy that he has access to. For Bob his optimal measurement involves minimising the probability of causing a photodetection event. This constitutes a minimum cost measurement with a cost matrix C with elements $c_{\phi,\theta}$. In a minimum cost measurement if a quantum state ρ_j occurs with prior probability p_j and we choose a measurement with a measurement operator Π_i and that obtaining result i when the state prepared was actually ρ_j carries a cost of C_{ij} [52]. The cost matrix C was obtained experimentally for the QDS system and is related to the encoding matrix shown in Figure 5.17. In the case where Bob is honest then the maximum probability of causing a photodetection event is given by $p_{original}$ and is equal to the largest diagonal elements of the cost matrix C. If the condition that

$p_{forgery} > p_{original}$ for a larger enough signature length L then it is possible to distinguish between honest and cheating scenarios using a statistical approach using Hoeffding's inequality. Hoeffding's inequality can be used to provide an upper bound on the probability that the sum of random variables deviates from its expected value [53]. The authentication and verification thresholds can be set to $s_a = 1/3g + p_{original}$ and $s_v = 2/3g + p_{original}$ where the gap $g = p_{forgery} - p_{original}$ plays a key role in the cheating probabilities. The value g was calculated to be 8.304×10^{-4} for a mean photon per pulse value of 0.16. The details of how of how the cost matrix C and the gap g were calculated is given in more detail in appendix A. In a passive attack strategy in the case of a cheating Bob the probability of forging equals the probability of Bob causing fewer than $s_v L$ photodetection events in Charlie's signal null-port. Using Hoeffding's inequalities the probability of forging is bounded by

$$\varepsilon_{forging} \leq 2\exp\left(-\frac{2}{9}g^2 L\right) \qquad \text{Equation (5.26)}$$

Similarly the probability for Bob and Charlie to reject a message from Alice in the case where all parties are honest is bounded by

$$\varepsilon_{robustness} \leq 2\exp\left(-\frac{2}{9}g^2 L\right) \qquad \text{Equation (5.27)}$$

5.12.6.2 Repudiation by Alice

In order for Alice to repudiate her signature she needs to create signature states so that Bob accepts and Charlie rejects the message when Bob forwards it to him or vice versa. Bob will accept a message if the number of photodetection events is less than $s_a L$ and Charlie will accept if his photodetection events is less than $s_v L$. If Alice is to succeed in cheating she needs that Charlie accumulates $(s_v - s_a)L$ more photodetection events than Bob. The probability of Alice causing one recipient to accept and the other to reject is given by

$$\varepsilon_{repudiate} = \left(\frac{1}{2}\right)^{(s_v - s_a)L} \qquad \text{Equation (5.28)}$$

5.13 Conclusions

This chapter has introduced the concept of digital signatures and shown how it can be used to sign a message in such a way that all users can authenticate the identity of a sender and verify that the message has been unaltered in transmission. The security of

such a classical digital scheme is based on the computational difficulty of reversing certain one-way functions but such an assumption cannot be guaranteed indefinitely in the future. Quantum computers or more realistically in the short term better algorithms could render such systems insecure overnight. In contrast quantum mechanics allows the construction of quantum one-way functions whose security is based not on computational difficulty but on the properties of quantum mechanics. In this chapter a quantum digital signature scheme has been described as well a working demonstrating of the system. The system operates at a clock frequency of 100 MHz and a wavelength of 850 nm using commercially available silicon single-photon detectors. Results from the system have been shown for 8 phase encodings using different values of $|\alpha|^2$ and also the effect of a cheating Alice.

One of the issues with the current setup is that it does not employ any form of quantum memory as the long term storage of qubits in a practical manner has yet to be demonstrated. Another issue with the current setup is that it is not practical to extend the distance between Charlie and Bob as they share a common arm of a Mach-Zehnder interferometer and maintaining the path length difference over a large distance of optical fibre would be impossible.

Increasing the clock rate of the system would also be beneficial. In addition to an increase in the bit rate which would be obtained the security of the system is also affected. To sign a particular message which meets a level of security given by the ε term in Equation (5.26), Equation (5.27) and Equation (5.28) requires a particular message length L. The longer L is, and hence the more secure the system is, the more time that is required to sign a message. Increasing the clock speed would decrease the time required.

5.14 Acknowledgements

The author would like to thank Dr Robert Collins for his help in the experimental design and build of the system presented in this chapter. The author would also like to thank Dr Erika Andersson who devised the original concept of an experimental implementation of quantum digital signatures and to Vedran Dunjko and Dr John Jeffers who performed the detailed security analysis for the system along with Dr Andersson.

References

[1] *"The Globus Toolkit 4 Programmer's Tutorial", 2004, http://gdp.globus.org/gt4-tutorial/multiplehtml/ch09s03.html, date accessed:3/7/2012*

[2] J. Katz, "*Digital Signatures (Advances in Information Security)"* 2010: Springer.

[3] O. Goldreich, "*P, NP, and NP-Completeness: The Basics of Computational Complexity"* 2010: Cambridge Univ Pr.

[4] W. Diffie and M. Hellman, "*New directions in cryptography"*. IEEE Transactions on information Theory, 1976. **22**(6): p. 644-654.

[5] A.G. Konheim, "*Computer security and cryptography"* 2007: Jossey-Bass.

[6] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone, "*Handbook of applied cryptography"* 1997: CRC.

[7] M.E. Briggs, "An introduction to the general number field sieve", Virginia Polytechnic Institute and State University, 1998

[8] C. Paar, J. Pelzl, and B. Preneel, "*Understanding cryptography: a textbook for students and practitioners"* 2010: Springer-Verlag New York Inc.

[9] R. Rivest, A. Shamir, and L. Adleman, "*A method for obtaining digital signatures and public-key cryptosystems"*. Communications of the ACM, 1978. **21**(2): p. 120-126.

[10] *"Constructing digital signatures from a one-way function", Technical Report CSL-98, SRI International,1979, date accessed:16/4/2012*

[11] D.E. Knuth, "*The Art of computer programming: Seminumerical algorithms"* 1973: Addison-Wesley.

[12] L. Grover. "*A fast quantum mechanical algorithm for database search"*. 1996. ACM New York, NY, USA.

[13] M.A. Nielsen and I.L. Chuang, "*Quantum Computation and Quantum Information"* 2000: Cambridge University Press.

[14] D.F. Xiaoyun Wang, Xuejia Lai, Hongbo Yu, "*Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD"*. Cryptology ePrint Archive, Report 2004/199, 2004.

[15] *"Flame malware collision attack explained", Microsoft,http://blogs.technet.com/b/srd/archive/2012/06/06/more-information-about-the-digital-certificates-used-to-sign-the-flame-malware.aspx, date accessed:20/6/2012*

[16] C. Zhou, G. Wu, X. Chen, and H. Zeng, "*"Plug and play" quantum key distribution system with differential phase shift"*. Applied Physics Letters, 2003. **83**: p. 1692.

[17] A. Bérut, A. Arakelyan, A. Petrosyan, S. Ciliberto, R. Dillenschneider, and E. Lutz, "*Experimental verification of Landauer/'s principle linking information and thermodynamics"*. Nature, 2012. **483**(7388): p. 187-189.

[18] C.C. Gerry and P.L. Knight, "*Introductory Quantum Optics"* 2005: Cambridge University Press.

[19] J. Machta, "*Entropy, information, and computation"*. American Journal of Physics, 1999. **67**: p. 1074-1077.

[20] E.A. Goldschmidt, M.D. Eisaman, J. Fan, S.V. Polyakov, and A. Migdall, "*Spectrally bright and broad fiber-based heralded single-photon source"*. Physical Review A, 2008. **78**(1): p. 013844.

[21] M.V. Volkenstein and A. Shenitzer, "*Entropy and information"* 2009: Birkhauser.

[22] D. Gottesman and H. Lo, "*Proof of security of quantum key distribution with two-way classical communications"*. IEEE Transactions on information Theory, 2003. **49**(2): p. 457-475.

[23] P.W. Shor and J. Preskill, "*Simple Proof of Security of the BB84 Quantum Key Distribution Protocol"*. Physical Review Letters, 2000. **85**(2): p. 441-444.

[24] C.P. Williams, "*Explorations in quantum computing"* 2010: Springer-Verlag New York Inc.

[25] P.W. Shor. "*Algorithms for quantum computation: discrete logarithms and factoring"*. in *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*. 1994.

[26] S. Barnett, "*Quantum information"* 2009: Oxford University Press, USA.

[27] R. Hardman, "*A toxicologic review of quantum dots: toxicity depends on physicochemical and environmental factors"*. Environmental health perspectives, 2006. **114**(2): p. 165.

[28] D. Levine and G.J. Monser, "*Polarization, Ghost, and Shading Effects in Dichroic Beam Splitters"*. Journal of the Optical Society of America, 1961. **51**(7): p. 783-789.

[29] D. Gottesman and I. Chuang, "*Quantum digital signatures"*. arXiv.org/abs/quant-ph/0105032, 2001.

[30] H. Buhrman, R. Cleve, J. Watrous, and R. De Wolf, "*Quantum fingerprinting"*. Physical Review Letters, 2001. **87**(16): p. 167902.

[31] E. Andersson, M. Curty, and I. Jex, "*Experimentally realizable quantum comparison of coherent states and its applications"*. J. Phys. A Phys Rev A, 2003. **74**: p. 022304.

[32] A.V. Sergienko, "*Quantum communications and cryptography"* 2005: CRC.

[33] S.M. Barnett, A. Chefles, and I. Jex, "*Comparison of two unknown pure quantum states"*. Physics Letters A, 2003. **307**(4): p. 189-195.

[34] I. Jex, E. Andersson, and A. Chefles, "*Comparing the states of many quantum systems"*. Journal of Modern Optics, 2004. **51**(4): p. 505-523.

[35] G. Weihs, M. Reck, H. Weinfurter, and A. Zeilinger, "*Two-photon interference in optical fiber multiports"*. Physical Review A, 1996. **54**(1): p. 893-897.

[36] R.J. Glauber, "*The Quantum Theory of Optical Coherence"*. Physical Review, 1963. **130**(6): p. 2529-2539.

[37] R. Loudon, "*The Quantum Theory of Light"* 2000: Oxford University Press.

[38] M. Fox, "*Quantum optics: an introduction"* 2006: Oxford University Press.

[39] E. Andersson, M. Curty, and I. Jex, "*Experimentally realizable quantum comparison of coherent states and its applications"*. Physical Review A, 2006. **74**(2): p. 022304.

[40] B. Julsgaard, J. Sherson, J.I. Cirac, J. Fiurasek, and E.S. Polzik, "*Experimental demonstration of quantum memory for light"*. Nature, 2004. **432**(7016): p. 482-486.

[41] J.V. Neumann, "*Mathematical Foundations of Quantum Mechanics"* 1996: Princeton University Press.

[42] A.D. Kersey, A. Dandridge, and A.B. Tveten, "*Dependence of visibility on input polarization in interferometric fiber-optic sensors"*. Optics Letters, 1988. **13**(4): p. 288-290.

[43] *"2.56 Gbps VCSEL and Laser Driver", MAXIM, San Jose, California U.S.,2004, http://datasheets.maxim-ic.com/en/ds/MAX3996.pdf, date accessed:28/6/2012*

[44] G.S. Buller and R.J. Collins, "*Single-photon generation and detection"*. Measurement Science and Technology, 2010. **21**: p. 012002.

[45] P. Maurer, G. Kucsko, C. Latta, L. Jiang, N. Yao, S. Bennett, F. Pastawski, D. Hunger, N. Chisholm, and M. Markham, "*Room-Temperature Quantum Bit Memory Exceeding One Second"*. Science, 2012. **336**(6086): p. 1283-1286.

[46] M. Steger, K. Saeedi, M. Thewalt, J. Morton, H. Riemann, N. Abrosimov, P. Becker, and H.J. Pohl, "*Quantum Information Storage for over 180 s Using*

Donor Spins in a 28Si "Semiconductor Vacuum"". Science, 2012. **336**(6086): p. 1280-1283.

[47] P. Townsend, J. Rarity, and P. Tapster, "*Single photon interference in 10 km long optical fibre interferometer".* Electronics Letters, 1993. **29**(7): p. 634-635.

[48] Z. Yuan and A. Shields, "*Continuous operation of a one-way quantum key distribution system over installed telecom fibre".* Optics Express, 2005. **13**(2): p. 660-665.

[49] *"PC-based time interval analyser GT658", http://www.guidetech.com/gt-658, date accessed:10/5/2012*

[50] *"HydraHarp 400-multi channel picosecond event time", PicoQuant GmbH, Berlin, Germany,2011, http:// www.picoquant.com/datasheets/photon_counting/ HydraHarp400.pdf, date accessed:15/6/2012*

[51] D.R. Stephens, "*Phase-locked loops for wireless communications: digital, analog, and optical implementations"* 2002: Springer.

[52] E. Andersson, "*Optimal minimum-cost quantum measurements for imperfect detection".* arXiv:1201.0387, 2012.

[53] W. Hoeffding, "*Probability inequalities for sums of bounded random variables".* Journal of the American Statistical Association, 1963: p. 13-30.

Chapter 6
Conclusions and future work

6.1 Conclusions

Chapter 1 provided a very brief introduction to the field of classical and quantum cryptography and gave an outline of the structure of the thesis.

Chapter 2 provided a more in depth discussion of quantum key distribution (QKD), charting its development from its initial birth through to the current state of the art. Classical cryptography systems were first introduced and the potential security problems inherent in these systems, namely if quantum computers could become a reality, was discussed. This then led on to show how cryptography systems based on quantum mechanics can offer verifiably secure encryption, which is based solely on the physical laws of quantum mechanics. Chapter 2 also dealt with how QKD systems could be physically realised in the laboratory. The principles and ideas of single-photon generation and detection were described together with time-correlated single-photon counting, used for the detection of faint repetitive optical signals.

Chapter 3 introduced a QKD system that utilised a single-photon source (SPS) for security enhancement. Using such a light source in a QKD system potentially offers substantial increase in security, as a SPS is robust against the photon number splitting attack unlike weak coherent pulses (WCP), and hence an increase in bit. If QKD is to become a widespread technology then the cheap and easy integration into existing classical communication networks is vital. The challenge involves trying to co-propagate a faint quantum signal with a much more intense classical signal, all in the same channel The system in this Chapter operated at a wavelength of 850 nm and offers the possibility that quantum data can coexist with classical data channels as they are spectrally well separated from each other. The SPS itself used a semiconductor quantum dot contained in a micropillar cavity, emitting at a wavelength of 895 nm, and optically excited at a pulse repetition rate of 40 MHz. The system used a polarisation encoding implementation of the BB84 protocol, the results of which have been successfully published in reference [1]. The highest emission rate leaving Alice was ~16 kHz with a $g^{(2)}(0)$ of 0.85. This enabled key generation to be successful over 2 km giving ~65 bits/s. Although transmission over 2 km may seem short compared to

long haul telecommunication distances, it does offer the potential for use in metropolitan telecommunications access links, which the International Telecommunication Union (ITU) recommends be no longer than 20 km [2].

Chapter 4 introduced an environmentally robust, gigahertz clocked, phase encoding QKD system. Phase encoding was implemented using unbalanced Mach-Zehnder interferometers. The aim of the research was to demonstrate a QKD system, which by using novel techniques, is robust against environmental fluctuations. This novel solution was used to eliminate random fluctuations in the intrinsic birefringence of the quantum channel, which is composed of standard telecoms fibre. These fluctuations are caused by environmentally induced stress, which can randomly alter the state of polarisation of light travelling through the quantum channel. This random polarisation evolution would be detrimental to the interferometric visibility and would result in larger encoding errors. The technique used a light source that has been deliberately depolarised, which eliminates birefringence effects in the fibre and allows the receiver to use passive optical components to make a random basis set selection. This depolarising technique reduces the complexity required in the receiver and eliminates active components, commonly used in other QKD systems, which can thermally destabilise the interferometers. The success of this depolarising method was demonstrated for the system by generating a key, operating completely autonomously over the course of 24 hours, over a 2 km fibre reel. The system securely generated keys for over 19 hours with an average bit rate of 16 kbits/s.

Chapter 4 also made the most comprehensive comparison of detectors in any QKD system published to date [3], looking at a variety of thick and thin junction Si single-photon detectors (SPAD) together with a superconducting nanowire device (SSPD). The goal was to investigate how various detector parameters, including timing jitter, detector efficiency and dark count rate, can affect the net bit rate achievable from the system. This may help when engineering detectors for QKD systems when trying to maximum the performance of the system. To aid the analysis, a theoretical model was developed to show how the various detector parameters affect the characteristic quantum bit error rate and net bit rate verses distance curve. The model was in very good agreement with the experimental results, which showed that detectors with good timing jitter and reasonably good detection efficiency, such as the resonant cavity SPAD and the SSPD, gave the largest bit rate. Furthermore, the versatility of the model

was demonstrated by predicting how particular improvements in detector design and performance could increase the net bit rate, which might hopefully stimulate future detector development.

Chapter 5 introduced the concept of digital signatures and how they play a vital importance in modern electronic commerce. Ron Rivest was famously quoted as saying that "they may prove to be one of the most fundamental and useful inventions of modern cryptography" [4]. However, akin to all modern classical cryptography, the security relies on the unproven difficulty of reversing certain mathematical functions. If a computational efficient method could be found it would have a profound and dramatic effect on modern commerce and communication systems. Quantum digital signatures (QDS) seek to eliminate this problem by relying solely on principles of quantum mechanics for its security. The QDS system described in Chapter 5 enables two parties, Bob and Charlie, to receive a message so that they are able to authenticate and verify that a message was sent by Alice and that it was not interfered with in transmission. Quantum signatures were encoded onto the phase of coherent pulses of light, enabling Alice to select from a possible of eight quantum signatures states. By careful choice of the amplitude of her phase encoded coherent states, she can ensure that the states are non-orthogonal, thus ensuring unauthorised parties cannot gain information about the state. Phase encoding was implemented using unbalanced Mach-Zehnder fibre interferometers, similar to the approach adopted in Chapter 4, which makes it possible for the easy integration into current communication solutions. The experimental QDS system, which is the first of its kind in the world, proved its ability to detect certain cheating scenarios in which the sender can attempt to get one receiver to accept a message while the other to reject. This work will hopefully encourage other researchers and institutions to follow on from this work and develop other QDS protocols and experimental implementations.

In summary, the work detailed in this thesis has led to 1. the first experimental demonstration of quantum digital signatures [5], 2. an environmentally robust, short wavelength, gigahertz clock rate, quantum key distribution system capable of autonomous operation [6], 3. a general purpose theoretical model, capable of predicting how detector performance affects quantum information experiments [3] and finally, 4. a quantum key distribution test-bed using a single-photon source [1]. The experiments

outlined in the preceding chapters can and will form the basis of future experiments at Heriot-Watt and other institutions and research laboratories.

6.2 Future work

6.2.1 Quantum digital signatures

Chapter 5 looked at what is believed to be the first experimental demonstration of quantum digital signatures. However, due to the lack of practical and easily accessible quantum information storage, it was not possible to fully implement the QDS scheme originally proposed by Anderson *et al.*[7]. In that protocol, Charlie and Bob would have to store their quantum signature states, received from Alice, in quantum memory and later interference them with states generated by each receiver from the classical description of the quantum state sent from Alice. To overcome this problem a technique commonly used in phase encoding QKD systems was used, in which a reference pulse is phase modulated and time multiplexed with a reference pulse, using asymmetric double Mach-Zehnder interferometers[8]. For more than two phase encodings a phase modulator is required in the receiver's interferometer. The issue with this current setup is that for state discrimination, Bob/Charlie must receive his classical description of the quantum signature state (i.e. electrical signal to the phase modulator) at the same time as he receives the actual signature state sent by Alice. To remove the requirement for Bob/Charlie to employ active phase modulators to measure the received quantum state, the experimental setup shown in Figure 6.1 was proposed by the research group. The experimental arrangement for Alice to encode her signature states, and the system which enables Bob and Charlie to compare their quantum signature states received from Alice (i.e. the multiport), are almost identical to those employed in Chapter 5. The method by which Charlie and Bob measure the phase of the encoded photon differs slightly, in that a phase modulator is used. For each receiver a total of four demodulation interferometers are required for the case where Alice can select from a possible of 4 phase encodings. Each demodulation interferometer has one output designated for the vacuum pulse, while the remaining output is for detecting one of the available phase states 0 , $\pi/2$, π or $3\pi/2$

The ability of a receiver, either Charlie or Bob, to distinguish a signature state sent from Alice depends on the optical loss of the system. If a receiver was to try to distinguish a signature state sent from Alice, using only one of their demodulation interferometers in Figure 6.1, the losses incurred in the system compared to the system used in Chapter 5

would be approximately 14 dB higher. A demodulation interferometer outlined in Chapter 5 has ~10 dB loss while the system employing 4 interferometers with no active phase modulator is estimated to have a loss of ~ 6 dB per each demodulation interferometer. In terms of the security parameters of the QDS system, there is an exponential dependence on the number of pulses required to sign a single bit, therefore, the loss of the system can be crucial. The next generation of the experiment could look at increasing the gated bit rate from the system while maintaining the same clock rate.

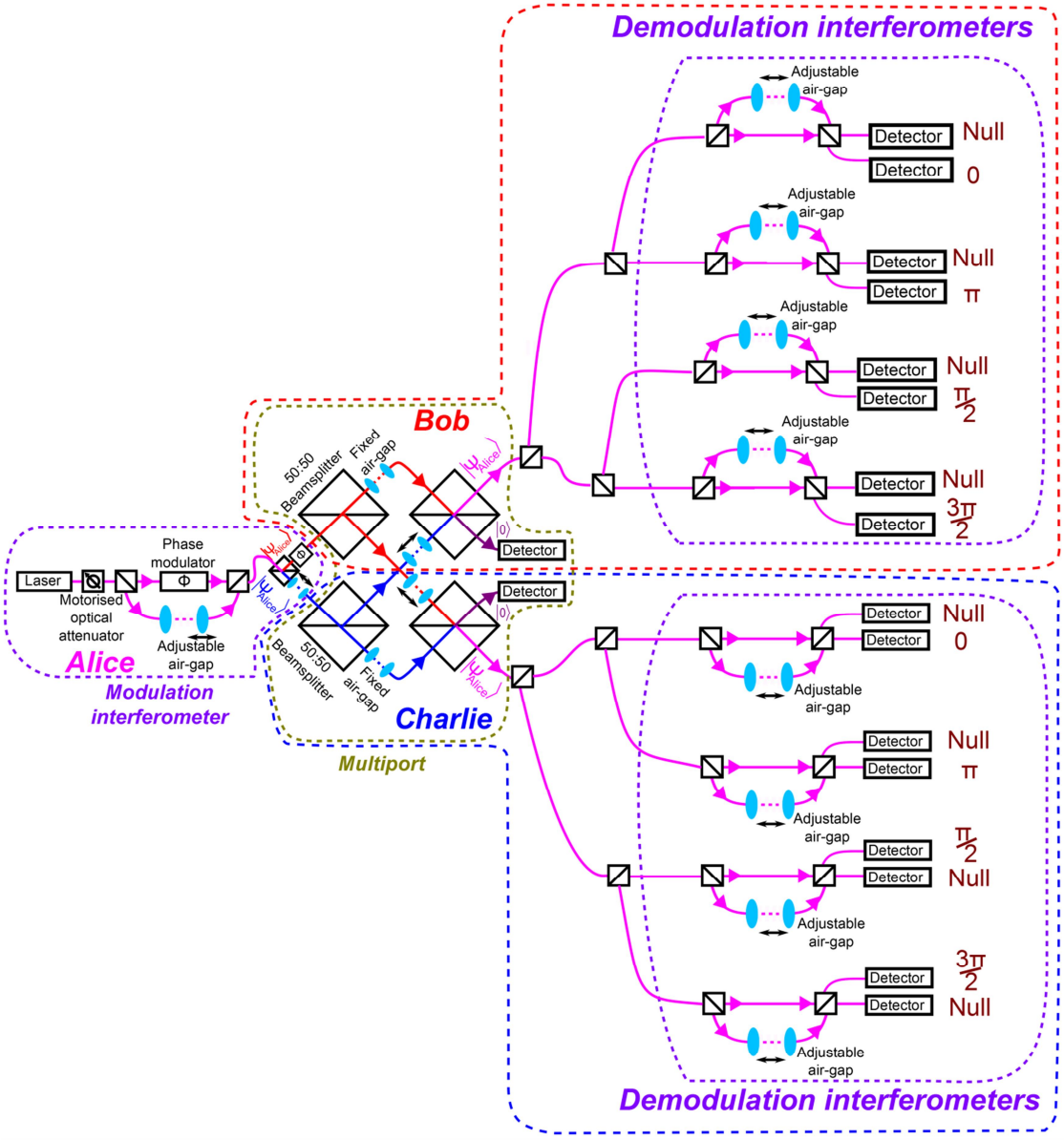

Figure 6.1. Scheme for quantum digital signatures with unambiguous state discrimination. Both Charlie's and Bob's phase demodulation apparatus contains 4 interferometers designated for measuring one of the 4 phase states 0, $\pi/2$, π and $3\pi/4$. As in Chapter 5 the multiport symmetrises the states sent by Alice which guarantees against repudiation by Alice.

The unbalanced Mach-Zehnder approach to phase encoding, which uses a phase modulated pulse, time multiplexed with a reference pulse, results in photons which do not experience any interference (described in more detail in Chapters 4 and 5). These photons do not contribute to any generated key and are time gated out using software. However, using polarisation routing techniques, shown by Marand and Townsend [9], photons are forced to take interfering paths only in the double Mach-Zehnder chain, thereby eliminating the non-interfering pulses. Using the theoretical model described in Chapter 4, it is estimated that by using this technique the time gated bit rate could be increased by a factor of ≈2.4.

Another possible QDS experimental implementation is shown in Figure 6.2, which implements a slightly different QDS protocol. In this arrangement the multiport has been removed and Charlie and Bob are connected to Alice by a single optical fibre each. This removes the issue of the two receivers needing to be in very close proximity to each other.

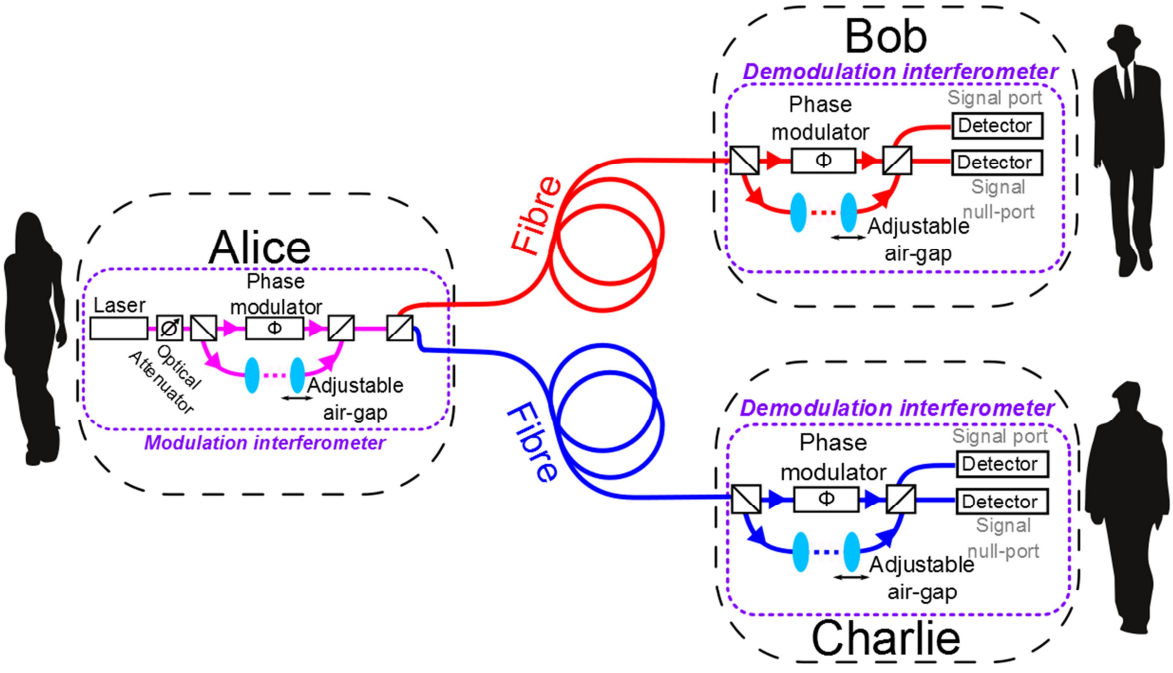

Figure 6.2. Experimental arrangement for the "sparse encoding" scheme for QDS. In this modified QDS scheme Alice sends a sequence of states to Charlie and Bob who after the states have been received asks Alice to reveal all but one element of the sequence. Alice has no a priori *knowledge of the choice Charlie and Bob make. The revealed parts of the sequence are used to check if the received states for both parties are the same while the sequence states which has not been revealed can be used for the quantum signature.*

The phase encoding and decoding of optical pulses uses the same principles as described in Chapter 4. In this layout, Alice sends a sequence of encoded pulses to Charlie and Bob, in which they agree on a chosen position in the sequence and ask Alice to reveal the classical description of the remaining states. As the majority of the sequence is used to check whether the states sent to both parties are the same, with only one state of the sequence retained for the signature, the scheme can be thought of as a "sparse encoding" method. However, one of the issues with this scheme is that it requires quantum memory to be implemented. The security of the system requires quantum memory which can hold the states for a duration of the order of twice the transit time between Alice and Bob/Charlie. Instead of measuring the states as soon as they arrive, Charlie and Bob should be able to store their states until they have a significant number and then perform measurements based on permutations of their received states. In principle, this could be achieved by adding long reels of fibre into the receiver, but maintaining the path length in fibre interferometers to within a wavelength of the source would be very challenging.

6.2.2 Possible future QKD work

The progress in experimental quantum key distribution has been rapid since it was first demonstrated close to 30 years ago. Using various implementations, the desire of researchers was to extend the distance over which keys could be generated and also the number of bits sent. Future work in this field could look at cryptographic protocols other than BB84, such as distributed phase reference protocols and continuous variable protocols, which were described in more detail in Chapter 2. The distributed phase reference protocol looks attractive as it is tolerant to the photon number splitting attack. In 2010, Lo *et al.* [10] described a measurement-device-independent (MDI) protocol, which uses a combination of decoy states technology together with approaches in entanglement based QKD protocols and is described in more detail in the next section.

6.2.3 Measurement-device-independent QKD

One area of possible future research, which at the time of writing is being investigated, is a newly proposed QKD scheme by Lo *et al.*, called measurement-device-independent (MDI) QKD[10]. A diagram of the proposed scheme is shown in Figure 6.3 and is designed to be immune from QKD hacking attacks based on imperfect devices, recently demonstrated by Lydersen *et al.*[11]. MDI QKD has the potential to double the transmission distance that can be covered over other QKD systems using conventional

laser diodes. In MDI QKD, both Alice and Bob are transmitters and the measurement procedure can be performed by an untrusted third party. In this scheme, Alice and Bob use decoy states, randomly preparing four possible BB84 polarisation encodings using weak coherent pulses, and then sends the state onto an untrusted third party called Charlie. Charlie performs a Bell state measurement which projects the incoming photons into a Bell state [12]. The rectilinear basis set (vertical, horizontal) is used as the key generation basis, while the diagonal basis set (45º, 135º) is used for testing only. Once the quantum communication has been completed, Charlie announces events where he obtained a successfully result, as well as the measurement result itself. Alice and Bob keep those events in which Charlie was successful and discard the rest. Using an authenticated public channel, Alice and Bob select events in which they used the same basis set as in their transmission. In Lo *et al.* they simulated the distance over which the MDI QKD scheme could operate. Using a value of 14.5% for Charlie's detector efficiency and transmittance of optical components, key generation could in theory be successfully completed up to a channel loss of 40 dB, which equates to about 200 km if the loss coefficient of the quantum channel is 0.2 dB/km. One of the practical difficulties in implementing MDI QKD is the ability to generate indistinguishable photons from two independent laser sources. Lo *et al.* demonstrated in their paper how this was achievable. They used one continuous wave (CW) laser emitting at a wavelength of 1550 nm, and one CW laser whose emission wavelength could be temperature tuned, both of which are commercially available. The lasers were used to create two optical pulses with a full-width half-maximum (FWHM) of 200 ps using intensity modulators. The spectral bandwidth of such optical pulses is 5 GHz. This is much larger than the central frequency mismatch between the two laser sources, in which the central wavelength of one of the laser sources can be tuned in steps of 0.1 pm. The Hong-Ou-Mandel (HOM) effect [13] was demonstrated, a phenomenon in which anti-correlations are observed in the output mode when two photons interfere on a 50:50 beamsplitter. Lo *et al.* managed to observe a HOM dip of 0.534, calculated using the normalised coincidence rate, $C = C_p / (C_1 C_2)$, where C_p is the probability of simultaneous clicks on both detectors and C_1 and C_2 are the photodetection count rates on the output of the 50:50 beamsplitter. In theory, when the two photons perfectly overlap in space they become indistinguishable and the coincidence rate should drop to a minimum value.

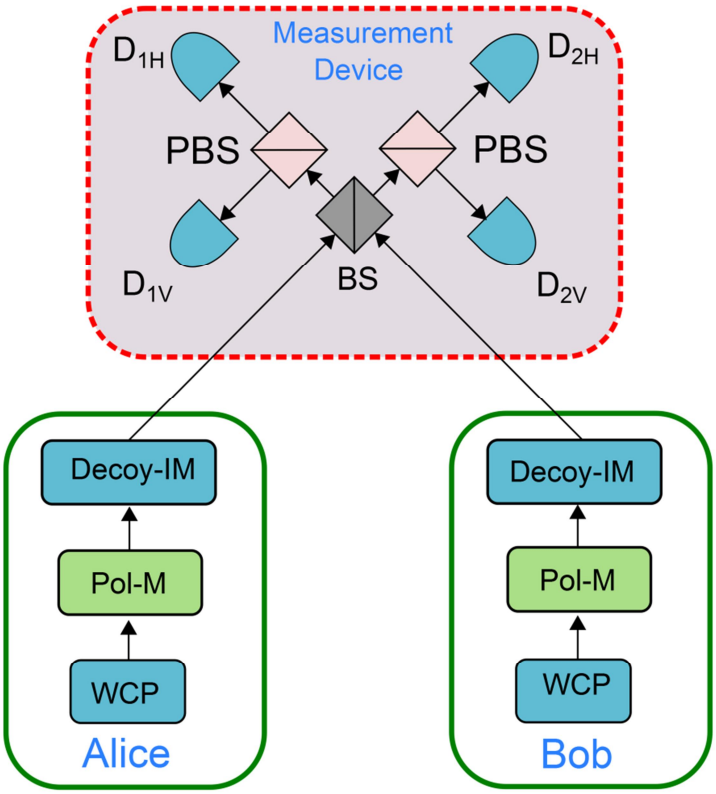

Figure 6.3. Schematic of MDI QKD system. Alice and Bob independently and randomly prepared4 BB84 polarisation states via their polarisation modulators (Pol-M). Decoy states are prepared by Alice and Bob by intensity modulators. Photons from Alice and Bob interfere at the 50:50 beam splitter (BS). At the outputs of the BS a polarisation beam splitter (PBS) transforms the incident photons in the horizontal (H) for vertical basis sets. If the Bell state measurement is successful two detector clicks are observed corresponding to detector designated for orthogonal polarisation. A detection click in D_{1H} and D_{2V} or D_{1V} and D_{2H} indicate the Bell state $|\psi^-\rangle = 1/\sqrt{2}\,(|HV\rangle - |VH\rangle)$ while a detector click in D_{1H} and D_{1V} or D_{2H} and D_{2V} indicates the state $|\psi^+\rangle = 1/\sqrt{2}\,(|HV\rangle + |VH\rangle)$ [10].

6.2.4 Future prospects for single-photon sources in quantum information

Although interest in using single-photon sources for applications in QKD may be waning in recent years, due to the development of decoy state protocols, the wider field of quantum information still requires efficient SPS. In 2001, Knill *et al.* [14] showed that for efficient quantum information processing, linear optics are sufficient as opposed to using non-linear effects, provided the photons are quantum mechanically indistinguishable. They described a controlled-sign flip gate through the teleportation of quantum states. The fidelity of the teleportation critically depends on the indistinguishability of photons emitted from a source, a property that can be obtained by using a SPS.

Another possible future use for SPS is in the area of quantum repeaters. Distributing quantum states over long distances is limited by photon loss. However Briegel *et al.* proposed an elegant solution to use entanglement to build a quantum repeater [15]. The idea involves dividing the overall transmission distance into individual smaller sections, distributing the entanglement in each section and then repeatedly swapping the entanglement between neighbouring links until the complete distance is covered. The proposed scheme requires a source of heralded photon pairs to operate. The entanglement distribution rate is dramatically increased if a SPS is used, as multiphoton emission increases the errors during the entanglement swapping operation.

Future development of SPS will aim for greater collection efficiencies and device integration for quantum-enabled technologies in information processing and communications. Davanço *et al.* demonstrated a room temperature operation, silicon heralded single-photon source, at the telecommunications band of 1550 nm through four wave mixing. This type of work aims to provide quantum photonic chips that can integrate single-photon sources with waveguide quantum photonic circuits and single photons detectors, all on the same silicon chip [16]. Other groups have continued to look at coloured centres in diamond with Mizuochi *et al.* demonstrating an electrically driven single-photon source based on a single neutral nitrogen-vacancy centre in a diamond diode structure [17]. Other research groups are looking at coupling quantum dots to a photonic crystal waveguide, where light slow-down effects can enhance the light-matter coupling strength, allowing efficient channelling of single photons from a quantum dot into a photonic crystal mode [18]. There is also much interest in generating entangled photons on demand and there is on-going work to eliminate fine-structure splitting effects in quantum dots via electric and strain fields [19] [20].

With regard to future advances in single-photon detector technology, there is interest in further improvements in single-photon avalanche photodiodes (SPADs) at telecoms wavelengths. One of the drawbacks of InP/InGaAs detectors is the phenomenon of afterpulsing, described in Chapter 2. The quality of the material plays a major role in the density of defects that lead to trapping centres, which in turn results in afterpulsing. This can limit the usefulness of these detectors in photon-counting applications at high repetition rates. It is believed that the trapping centres are located in the InP layer but its exact nature is not fully understood. Current research is looking at improvements in

material growth in addition to limiting the current that flows through these devices using self-differencing circuits [21].

Current research in silicon based SPADs is looking at complementary metal–oxide–semiconductor (CMOS) fabricated devices, that can integrate both the detector and the associated quenching circuits onto the same chip, which has the benefit of reduced size and low parasitic capacitance. However CMOS technology is not fully optimised for SPAD fabrication. Planar detector technology is now looking at identifying and removing all possible sources of contamination in the detector processing such as transition metals. Decreasing the electric field in the p-n junction depletion region is also being examined to reduce band-to-band tunnelling and the field-enhanced tunnelling of carriers. With careful design, devices with reduced dark counts, higher photon detection efficiencies and lower timing jitter may be achieved [22].

References

[1] R. Collins, P. Clarke, V. Fernandez, K. Gordon, M. Makhonin, J. Timpson, A. Tahraoui, M. Hopkinson, A. Fox, and M. Skolnick, "*Quantum key distribution system in standard telecommunications fiber using a short wavelength single photon source"*. Journal of Applied Physics, 2010. **107**(7): p. 073102-073102-6.

[2] *"Recommendation G.983.1. Series G: Broadband optical access systems based on Passive Optical Networks (PON)", http://www.itu.int/rec/T-REC-G.983.1-200501-I/en, date accessed:15/8/2012*

[3] P.J. Clarke, R.J. Collins, P.A. Hiskett, M.J. García-Martínez, N.J. Krichel, A. McCarthy, M.G. Tanner, J.A. O'Connor, C.M. Natarajan, S. Miki, M. Sasaki, Z. Wang, M. Fujiwara, I. Rech, M. Ghioni, A. Gulinatti, R.H. Hadfield, P.D. Townsend, and G.S. Buller, "*Analysis of detector performance in a gigahertz clock rate quantum key distribution system"*. New Journal of Physics, 2011. **13**: p. 075008.

[4] R.L. Rivest, "*Cryptography"*, in *Handbook of theoretical computer science (vol. A)*1990, MIT Press. p. 617-755.

[5] P.J. Clarke, R.J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G.S. Buller, "*Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light"*. Nature Communications, 2012. **3**: p. 1174.

[6] P.J. Clarke, R.J. Collins, P.A. Hiskett, P.D. Townsend, and G.S. Buller, "*Robust gigahertz fiber quantum key distribution"*. Applied Physics Letters, 2011. **98**(13): p. 131103-131103-3.

[7] E. Andersson, M. Curty, and I. Jex, "*Experimentally realizable quantum comparison of coherent states and its applications"*. Physical Review A, 2006. **74**(2): p. 022304.

[8] P. Townsend, "*Secure key distribution system based on quantum cryptography"*. Electronics Letters, 1994. **30**(10): p. 809-811.

[9] C. Marand and P. Townsend, "*Quantum key distribution over distances as long as 30 km"*. Optics Letters, 1995. **20**(16): p. 1695.

[10] H.-K. Lo, M. Curty, and B. Qi, "*Measurement-Device-Independent Quantum Key Distribution"*. Physical Review Letters, 2012. **108**(13): p. 130503.

[11] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "*Hacking commercial quantum cryptography systems by tailored bright illumination"*. Nature Photonics, 2010. **4**(10): p. 686-689.

[12] M.A. Nielsen and I.L. Chuang, "*Quantum Computation and Quantum Information"* 2000: Cambridge University Press.

[13] C.K. Hong, Z.Y. Ou, and L. Mandel, "*Measurement of subpicosecond time intervals between two photons by interference"*. Physical Review Letters, 1987. **59**(18): p. 2044-2046.

[14] E. Knill, R. Laflamme, and G.J. Milburn, "*A scheme for efficient quantum computation with linear optics"*. Nature, 2001. **409**(6816): p. 46-52.

[15] H.J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, "*Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication"*. Physical Review Letters, 1998. **81**(26): p. 5932-5935.

[16] M. Davanço, J.R. Ong, A.B. Shehata, A. Tosi, I. Agha, S. Assefa, F. Xia, W.M.J. Green, S. Mookherjea, and K. Srinivasan, "*Telecommunications-band heralded single photons from a silicon nanophotonic chip"*. Applied Physics Letters, 2012. **100**(26): p. 261104-261104-4.

[17] N. Mizuochi, T. Makino, H. Kato, D. Takeuchi, M. Ogura, H. Okushi, M. Nothaft, P. Neumann, A. Gali, and F. Jelezko, "*Electrically driven single-photon source at room temperature in diamond"*. Nature Photonics, 2012. **6**(5): p. 299-303.

[18] T. Lund-Hansen, S. Stobbe, B. Julsgaard, H.T. Nielsen, T. Sünner, M. Kamp, A. Forchel, and P. Lodahl, "*Experimental realization of highly efficient broadband coupling of single quantum dots to a photonic crystal waveguide"*. Physical review letters, 2008. **101**(11).

[19] M. Ghali, K. Ohtani, Y. Ohno, and H. Ohno, "*Generation and control of polarization-entangled photons from GaAs island quantum dots by an electric field"*. Nature Communications, 2012. **3**: p. 661.

[20] C.E. Kuklewicz, R.N.E. Malein, P.M. Petroff, and B.D. Gerardot, "*Electro-elastic tuning of single particles in individual self-assembled quantum dots"*. Nano letters, 2012. **12**(7): p. 3761-3765.

[21] M.A. Itzler, X. Jiang, M. Entwistle, K. Slomkowski, A. Tosi, F. Acerbi, F. Zappa, and S. Cova, "*Advances in InGaAsP-based avalanche diode single photon detectors"*. Journal of Modern Optics, 2011. **58**(3-4): p. 174-200.

[22] A. Gulinatti, I. Rech, P. Maccagnani, M. Ghioni, and S. Cova. "*Improving the performance of silicon single-photon avalanche diodes"*. in *SPIE Defense, Security, and Sensing*. 2011. International Society for Optics and Photonics.

Appendix A

In Chapter 5 an experimental quantum digital signatures system was first introduced. The security analysis presented in that chapter made use of a minimum cost measurement for an attempted forgery by one of the recipients. The cost matrix realised by in the experimental set-up using 8 differing phase states and with average photon number of $|\alpha|^2 = 0.16$ per pulse is given by

$$C = \begin{pmatrix} 3.89 & 4.40 & 5.24 & 5.95 & 6.35 & 6.00 & 5.29 & 4.39 \\ 4.56 & 3.88 & 4.43 & 5.29 & 6.04 & 6.39 & 6.02 & 5.20 \\ 5.28 & 4.60 & 3.89 & 4.42 & 5.29 & 6.02 & 6.37 & 5.95 \\ 5.68 & 5.22 & 4.58 & 3.90 & 4.40 & 5.24 & 5.91 & 6.30 \\ 6.36 & 5.68 & 5.27 & 4.59 & 3.89 & 4.43 & 5.24 & 6.01 \\ 5.62 & 6.36 & 5.66 & 5.23 & 4.57 & 3.89 & 4.41 & 5.30 \\ 5.26 & 5.68 & 6.40 & 5.70 & 5.22 & 4.60 & 3.88 & 4.40 \\ 4.61 & 5.24 & 5.65 & 6.36 & 5.68 & 5.22 & 4.56 & 3.88 \end{pmatrix} \times 10^{-3}$$

The cost matrix is related to the values presented in Figure 5.18 in chapter 5. Whereas in Figure 5.18, the values shown were the encoding errors, the cost matrix values are calculated by dividing the total number of signal null-port counts by the total number of pulses (including vacuum) emitted by Alice during the duration of the measurement (or equivalently clock frequency multiplied by measurement duration). As in Figure 5.18 in chapter 5, the diagonal elements represent the cases when receiver measures using the same phase as set by Alice, the off-diagonal elements represent the cases where a different phase is employed. The number of pulses reaching a receiver's signal null-port is, roughly speaking, proportional to the intensity of the incident light, and the cost matrix elements will therefore scale linearly with $|\alpha|^2$.

In the most general case for an arbitrary cost matrix, the computation of the optimal measurement is difficult. However if the cost matrix C is replaced by a cost matrix where each entry is less than or equal to the entries of the original cost matrix (an element dominated matrix), the overall cost of the optimal transform can only decrease. In the ideal case, where the experiment is completely symmetric, the cost matrix C is circulant and symmetric. The symmetrised and circularised cost matrix which lower bounds the original cost matrix is characterised by its first row which is given by

$$C'_{row} = (3.88, 4.39, 5.22, 5.91, 6.30, 5.91, 5.22, 4.39) \times 10^{-3}$$

and the upper bounding symmetrised and circularised matrix is characterised by the row

$$C''_{row} = (3.90, 4.43, 5.30, 6.04, 6.39, 6.04, 5.30, 4.43) \times 10^{-3}$$

For both lower and upper bounding cost matrices it was numerically checked if the fourth Helstrom criterion is satisfied [1], so in both cases, the minimum cost measurement is realised by the square-root measurement, and the costs are given by $\text{cost}_{lower} = 4.70 \times 10^{-3}$ and $\text{cost}_{upper} = 4.76 \times 10^{-3}$. For the worst case scenario, it is necessary to take the largest diagonal element of the actual cost matrix as p_{honest}, which is 3.9×10^{-3}, and the lower and upper bounds on the gap g are $g_{lower} = 8.03 \times 10^{-4}$ and $g_{upper} = 8.64 \times 10^{-4}$, This demonstrates that the bounding technique yields a useful bound. Thus the security of the QDS system can be characterised by the lower bound on the gap $g_{lower} = 8.03 \times 10^{-4}$.

Acknowledgments

The author would like to acknowledge that the theoretical security analysis presented in this appendix was performed by Vedran Dunjko, Dr Andersson and Dr John Jeffers.

References

[1] C.W. Helstrom, "*Quantum detection and estimation theory*". Journal of Statistical Physics, 1969. **1**(2): p. 231-252.